量子計算入門(講義ノート)

AUTHOR(S):

中原, 幹夫

CITATION:

中原, 幹夫. 量子計算入門(講義ノート). 物性研究 2005, 83(6): 699-786

ISSUE DATE:

2005-03-20

URL:

http://hdl.handle.net/2433/110153

物性研究　83－6（2005－3）

講義ノート

量子計算入門[1, *)]

近畿大学 理工学部　　中原 幹夫 [2]

(2005年1月17日受理)

1　はじめに

現在のディジタル情報，ディジタル計算（以下，古典情報，古典計算という）は0と1の値をとるビット (bit) をその単位とする．一方，今から解説する量子情報，量子計算では0と1の重ね合わせ状態である量子ビット (qubit) を単位とする．それにより古典的なディジタル情報を凌駕する情報処理がいかに可能となるか，以下に解説したい．情報科学や数学など，物理を専攻とする人以外にも理解できるよう心がけたがため，物理を専門とする読者にはまだるっこしいところもあるかもしれない．適当に取捨選択されたい．

講義内容は標準的なもので，文末にあげた参考文献 [1, 2, 3, 4, 5, 6, 7] などから適宜題材を選んだ．最終章以外において著者のオリジナルな寄与は例だけであるが，これらの例が読者の理解の助けとなることを望む．また，量子誤り訂正符号など多くの重要なテーマに触れることができなかったが，これらに関しては上述の文献を参照されたい．講義では理論の概略を述べた後，物理系における量子ビットの実現をいくつか紹介したが，最終章にその中の一つNMR量子コンピュータの概略を述べ，あわせて我々の最近の実験も紹介する．

以下で記号 $\mathbb{N}$: 自然数，$\mathbb{Z}$: 整数，$\mathbb{Q}$: 有理数，$\mathbb{R}$: 実数，$\mathbb{C}$: 複素数を用いる．数の集合の間の関係 $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ に注意せよ．本講義では，主に複素ベクトル空間を扱う．また，3つのPauliスピン行列と単位行列を

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

で定義する．$K = \mathbb{C}$ または $\mathbb{R}$ を行列要素とする n 次正方行列の集合を $M(n, K)$ と表す．

2　線型代数の補足

本節ではエルミート行列のスペクトル分解，行列やベクトル空間のテンソル積など，以下用いる線型代数に関して補足をする．ベクトル空間の初歩は既知とする．

[1] この原稿は，2003年10月8,9,10日に京都大学理学研究科で行った集中講義ノートに大幅に加筆訂正を行ったものである．

[2] E-mail: nakahara@math.kindai.ac.jp

*) 本稿は、編集部の方から特にお願いして執筆していただいた記事である。

2.1　ブラとケット

2.1.1　ケット・ベクトル

複素数体 $\mathbb{C}$ 上のベクトル空間 $V(n,\mathbb{C})=\mathbb{C}^n$ を考える．この元を**ケット（ベクトル）**といい

$$|x\rangle=\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}=(x_1,x_2,\ldots,x_n)^T\quad(x_k\in\mathbb{C})$$

のように複素数を n 個並べて表す．T は転置操作を表す．自然数 n を $V(n,\mathbb{C})$ の次元という．ケットの和 $|x\rangle+|y\rangle$ とスカラー倍 $a|x\rangle$ は成分ごとに与えられる．線型結合 $c_1|x\rangle+c_2|y\rangle$ を $|c_1x+c_2y\rangle$ とかくこともある．

2.1.2　線型独立，線型従属，基底ベクトル

k 個のベクトルの組 $\{|x_1\rangle,\ldots,|x_k\rangle\}$ が与えられたとき $\sum_{i=1}^{k}c_i|x_i\rangle=0$ の解が $c_1=c_2=\ldots=c_k=0$ しかないとき，$\{|x_1\rangle,\ldots,|x_k\rangle\}$ は**線型独立**，それ以外のときは**線型従属**という．ゼロベクトル $|0\rangle=(0,\ldots,0)^T$ を含む組は常に線型従属である．$\mathbb{C}^n$ において線型独立なベクトルは高々 n 個であり，$n+1$ 個以上のベクトルは常に線型従属となる．

問 2.1　2つのベクトル

$$|v_1\rangle=\begin{pmatrix}x\\y\\3\end{pmatrix},\ |v_2\rangle=\begin{pmatrix}2\\x-y\\1\end{pmatrix}$$

が線型独立となる条件を求めよ．

$\mathbb{C}^n$ において n 個の線型独立なベクトル $\{|v_i\rangle\}$ が与えられると，任意の $|x\rangle\in\mathbb{C}^n$ は $|x\rangle=\sum_{i=1}^{n}x_i|v_i\rangle$，$x_i\in\mathbb{C}$ と表される．$\{x_i\}$ を $|x\rangle$ の成分という．また $\{|v_i\rangle\}$ を $\mathbb{C}^n$ の基底，各 $|v_i\rangle$ を基底ベクトルという．

問 2.2　ベクトル

$$|v_1\rangle=\begin{pmatrix}1\\1\\1\end{pmatrix},\quad|v_2\rangle=\begin{pmatrix}1\\0\\1\end{pmatrix},\quad|v_3\rangle=\begin{pmatrix}1\\-1\\-1\end{pmatrix}$$

は $\mathbb{C}^3$ における基底であることを示せ．

2.1.3　線型関数，双対空間，ブラベクトル

$f:\mathbb{C}^n\to\mathbb{C}$ が

$$f(c_1|x\rangle+c_2|y\rangle)=c_1f(|x\rangle)+c_2f(|y\rangle),\quad\forall|x\rangle,|y\rangle\in\mathbb{C}^n,\forall c_1,c_2\in\mathbb{C}\tag{1}$$

を満たすとき f を**線型関数**という．線型関数は**ブラ（ベクトル）**

$$\langle\alpha| = (\alpha_1, \ldots, \alpha_n), \quad \alpha_i \in \mathbb{C} \tag{2}$$

で表される．ブラ $\langle\alpha|$ とケット $|x\rangle$ の内積を

$$\langle\alpha|x\rangle = \sum_{i=1}^{n} \alpha_i x_i \in \mathbb{C} \tag{3}$$

で定義する（これは通常の行列の積である）．するとこれが上の線形性を満たすことは直ちに確かめられる．逆に $\mathbb{C}^n$ の基底を $\{|v_i\rangle\}$ とすると，任意の線型関数は $f(|v_i\rangle) = \alpha_i$ を与えることによって定義される．すると

$$f(|x\rangle) = f(\sum x_i|v_i\rangle) = \sum x_i f(|v_i\rangle) = \sum \alpha_i x_i$$

となり，f が $\langle\alpha|$ と 1 : 1 に対応していることが分かる．

ブラベクトルの集合

$$\mathbb{C}^{n*} = \{\langle\alpha| = (\alpha_1, \ldots, \alpha_n) | \alpha_i \in \mathbb{C}\} \tag{4}$$

はそれ自身ベクトル空間の公理を満たす．これを**双対ベクトル空間**という．

ケット $|x\rangle \in \mathbb{C}^n$ が与えられたとき，それから自然にブラベクトル

$$|x\rangle \mapsto \langle x| = (x_1^*, \ldots, x_n^*) \in \mathbb{C}^{n*}, \tag{5}$$

が得られる．複素共役をとるのは $|x\rangle$ のノルムを $\|x\| = \sqrt{\langle x|x\rangle}$ で定義するためである．$\|x\|$ は非負実数である．実際 $\sqrt{\langle x|x\rangle} = [\sum_{i=1}^n x_i^* x_i]^{1/2} = \left[\sum_{i=1}^n |x_i|^2\right]^{1/2} \geq 0$ となる．これから 2 つのケット $|x\rangle, |y\rangle \in \mathbb{C}^n$ の内積が

$$\langle x|y\rangle = \sum_{i=1}^{n} x_i^* y_i \tag{6}$$

で定義される．定義から $\langle x|y\rangle = \langle y|x\rangle^*$ が成り立つ．

次の双線型性に注意せよ：

$$\langle x|c_1 y_1 + c_2 y_2\rangle = c_1\langle x|y_1\rangle + c_2\langle x|y_2\rangle, \tag{7}$$

$$\langle c_1 x_1 + c_2 x_2|y\rangle = c_1^*\langle x_1|y\rangle + c_2^*\langle x_2|y\rangle. \tag{8}$$

2.2 正規直交基底，完全性関係，射影演算子

基底の中でも特に便利なものは**正規直交基底** $\{|e_i\rangle\}$ である．これは

$$\langle e_i|e_j\rangle = \delta_{ij} \tag{9}$$

で定義される．明らかに $\{|e_i\rangle\}$ はこれだけでは決まらず，$\mathbb{C}^n$ ではユニタリー群 $\mathrm{U}(n)$ の，$\mathbb{R}^n$ では直交群 $\mathrm{O}(n)$ の自由度が残っている．以下，特に断らない限り基底は正規直交系にとる．

$|x\rangle = \sum_{i=1}^{n} x_i|e_i\rangle$ と $\langle e_j|$ の内積をとると $\langle e_j|x\rangle = \sum_{i=1}^{n} x_i\langle e_j|e_i\rangle = \sum_{i=1}^{n} x_i\delta_{ji} = x_j \to x_j = \langle e_j|x\rangle$ となり，成分 x_i が得られる．これを $|x\rangle$ に代入すると $|x\rangle = \sum_{i=1}^{n}\langle e_i|x\rangle|e_i\rangle = \sum_{i=1}^{n}|e_i\rangle\langle e_i|x\rangle$ が得られる．$|x\rangle$ は任意であるので**完全性関係**

$$\sum_{i=1}^{n}|e_i\rangle\langle e_i| = I_n \tag{10}$$

が得られた．I_n は n 次の単位行列である．

量子情報でしばしば用いられる基底は

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

や

$$|\to\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix},\ |\leftarrow\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

などである．$\sigma_z|0\rangle = |0\rangle, \sigma_z|1\rangle = -|1\rangle$, $\sigma_x|\to\rangle = |\to\rangle, \sigma_x|\leftarrow\rangle = -|\leftarrow\rangle$ である．

$\mathbb{C}^n$ のケットとブラの積 $|x\rangle\langle y|$ は $n\times n$ 行列となる．特に重要な行列に

$$P_k \equiv |e_k\rangle\langle e_k| \tag{11}$$

がある．これを $|e_k\rangle$ 方向の**射影演算子**という．P_k は $|v\rangle$ を $|e_k\rangle$ の方向に射影する．したがって $(|v\rangle - P_k|v\rangle) \perp |e_k\rangle$．実際，$\langle e_k|(|v\rangle - P_k|v\rangle) = \langle e_k|v\rangle - \langle e_k|e_k\rangle\langle e_k|v\rangle = 0$．射影演算子は以下の関係を満たす：

$$\text{(i)} \quad P_k^2 = P_k \tag{12}$$

$$\text{(ii)} \quad P_kP_j = 0 \quad (k \neq j) \tag{13}$$

$$\text{(iii)} \quad \sum_k P_k = I \quad \text{(完全性関係)} \tag{14}$$

例 2.1 $\mathbb{C}^2$ の正規直交基底

$$|e_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix},\ |e_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} i \\ 1 \end{pmatrix}$$

を考える．それぞれの射影演算子は

$$P_1 = |e_1\rangle\langle e_1| = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ i & 1 \end{pmatrix},\ P_2 = |e_2\rangle\langle e_2| = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$$

で，これらは完全性関係 $\sum_k P_k = I_2$ と直交関係 $P_1P_2 = 0.$ を満たす．各自 $P_k^2 = P_k$ を確かめよ．

2.2.1 Gram-Schmidt の直交化

射影演算子の応用として**Gram-Schmidt の直交化**を考える．$\mathbb{C}^n$ において，任意の k 個 $(k \leq n)$ の線型独立なベクトル $\{|v_i\rangle\}$ が与えられたとき，これから正規直交系 $\{|e_i\rangle\}$ を構成しよう．まず

$$|e_1\rangle = |v_1\rangle / \||v_1\rangle\|$$

とする．次に $|f_2\rangle = |v_2\rangle - |e_1\rangle\langle e_1|v_2\rangle$ とおくと，これは明らかに $|e_1\rangle$ と直交する; $\langle e_1|f_2\rangle = \langle e_1|v_2\rangle - \langle e_1|e_1\rangle\langle e_1|v_2\rangle = 0$．したがってこれを規格化して

$$|e_2\rangle = |f_2\rangle / \||f_2\rangle\|$$

が得られる．同様に j 番目のステップでは

$$|e_j\rangle = \frac{|v_j\rangle - \sum_{i=1}^{j-1}\langle e_i|v_j\rangle|e_i\rangle}{\||v_j\rangle - \sum_{i=1}^{j-1}\langle e_i|v_j\rangle|e_i\rangle\|}$$

が得られる．$\{|e_1\rangle, |e_2\rangle, \ldots, |e_k\rangle\}$ は $\mathbb{C}^n$ の k 次元部分ベクトル空間を張る．構成から $\{|e_i\rangle\}$ が $\{|v_i\rangle\}$ と同じ部分ベクトル空間を張ることは明らかであろう．

例 2.2

$$|v_1\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix}, |v_2\rangle = \begin{pmatrix} 2i \\ 4 \end{pmatrix}$$

とすると

$$|e_1\rangle = \frac{|v_1\rangle}{\||v_1\rangle\|} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$$

および

$$|f_2\rangle = \begin{pmatrix} 2i \\ 4 \end{pmatrix} - \frac{1}{2}(1, -i)\begin{pmatrix} 2i \\ 4 \end{pmatrix}\begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 3i \\ 3 \end{pmatrix},$$

から

$$|e_2\rangle = \frac{|f_2\rangle}{\||f_2\rangle\|} = \frac{1}{\sqrt{2}}\begin{pmatrix} i \\ 1 \end{pmatrix}.$$

問 2.3 Gram-Schmidt 法を用いて，下の $\{|v_1\rangle, |v_2\rangle\}$ と同一の 2 次元部分ベクトル空間を張る $\mathbb{C}^3$ の正規直交ベクトルを求めよ：

$$|v_1\rangle = (1, i, 1)^T, \ |v_2\rangle = (3, 1, i)^T.$$

2.3 線型演算子と行列表示，エルミート共役，エルミート行列，ユニタリー行列

写像 $\hat{A} : \mathbb{C}^n \to \mathbb{C}^n$ が任意の $|x\rangle, |y\rangle \in \mathbb{C}^n, c_k \in \mathbb{C}$ にたいし

$$\hat{A}(c_1|x\rangle + c_2|y\rangle) = c_1\hat{A}|x\rangle + c_2\hat{A}|y\rangle \tag{15}$$

を満たすとき $\hat{A}$ を**線型演算子**という．[3]正規直交系 $\{|e_k\rangle\}$ をとり $|v\rangle = \sum_{k=1}^{n} v_k|e_k\rangle \in \mathbb{C}^n$ を任意のベクトルとすると，線形性から $\hat{A}|v\rangle = \sum_k v_k\hat{A}|e_k\rangle$ となる．$\hat{A}|e_k\rangle \in \mathbb{C}^n$ であるから $\hat{A}|e_k\rangle = \sum_{i=1}^{n}|e_i\rangle A_{ik}$ と展開できる．これと $\langle e_j|$ の内積をとると $A_{jk} = \langle e_j|\hat{A}|e_k\rangle$ が得られる．これを与えられた基底に対する $\hat{A}$ の行列要素という．A_{ij} は基底の選び方に依存する．$A = (A_{ij})$ を与えられた基底に対する $\hat{A}$ の行列表示という．このとき完全性関係から

$$\hat{A} = \sum_{j,k}|e_j\rangle\langle e_j|\hat{A}|e_k\rangle\langle e_k| = \sum_{j,k} A_{jk}|e_j\rangle\langle e_k| \tag{16}$$

とあらわされる．

以下簡単のために線型演算子から ^ を省略し，その行列表示と区別せずに用いるが，複数の基底を同時に使う場合は，夫々の基底に対する行列表示に添え字をつけるなどして区別しなければならない．

定義 2.1 線型写像 $A : \mathbb{C}^n \to \mathbb{C}^n$ が与えられたとき，その**エルミート共役** $A^\dagger$ を

$$\langle u|A|v\rangle = \langle v|A^\dagger|u\rangle^* \quad \forall|u\rangle, |v\rangle \in \mathbb{C}^n \tag{17}$$

で定義する．ここに $*$ は複素共役．

定義から $\langle e_j|A|e_k\rangle = \langle e_k|A^\dagger|e_j\rangle^*$ であるから $(A^\dagger)_{jk} = A^*_{kj}$．同様にケット $|x\rangle$ にたいし $|x\rangle^\dagger = (x_1^*, \ldots, x_n^*) = \langle x|$ となる．このようにケットからブラを導く過程はエルミート共役をとるといってもよい．

定義 2.2 写像 $A : \mathbb{C}^n \to \mathbb{C}^n$ が $A^\dagger = A$ をみたすとき，A を**エルミート行列**という．このとき A の行列要素は $A_{ij} = A^*_{ji}$ を満たす．

$\{|e_i\rangle\}$ を $\mathbb{C}^n$ の正規直交基底とする．行列 $U : \mathbb{C}^n \to \mathbb{C}^n$ が $U^\dagger U = UU^\dagger = I_n$ を満たすとすると $|f_k\rangle = U|e_k\rangle$ も正規直交基底である．実際 $\langle f_j|f_k\rangle = \langle e_j|U^\dagger U|e_k\rangle = \langle e_j|e_k\rangle = \delta_{jk}$．また $\det U^\dagger U = \det U^\dagger \det U = |\det U|^2 = 1$ から $|\det U| = 1$ が得られる．

定義 2.3 線型写像 $U : \mathbb{C}^n \to \mathbb{C}^n$ が $U^\dagger = U^{-1}$ を満たすとき U を**ユニタリー行列**という．特に $\det U = 1$ であれば U は**特殊ユニタリー行列**という．

ユニタリー行列の集合 $\mathrm{U}(n) = \{U \in M(n,\mathbb{C})|\ U^\dagger = U^{-1}\}$ は行列の積に関し群となる．これを**ユニタリー群**という．また特殊ユニタリー行列の集合 $\mathrm{SU}(n) = \{U \in U(n)|\ \det U = 1\}$ を**特殊ユニタリー群**という．同様に実行列の集合 $\mathrm{O}(n) = \{O \in M(n,\mathbb{R})|O^{\mathrm{T}} = O\}$ を**直交群**，$\mathrm{SO}(n) = \{O \in \mathrm{O}(n)|\det O = 1\}$ を**特殊直交群**という．

問 2.4 $\mathrm{U}(n), \mathrm{SU}(n), \mathrm{O}(n), \mathrm{SO}(n)$ は実際群となることを示せ．

[3]一般に $\hat{A} : \mathbb{C}^n \to \mathbb{C}^m$ でもかまわない．そのときは $\hat{A}$ を表す行列は $m \times n$ 行列となる．

2.4 固有値，固有ベクトル

行列 A が与えられたとき $|v\rangle$ $(\neq |0\rangle)$ を「うまく」とって $A|v\rangle = \lambda|v\rangle$, $\lambda \in \mathbb{C}$ となるとき $|v\rangle$ を A の固有ベクトル，λ をその固有値という．固有ベクトルのノルムは固定できないが，常にそれを 1 に規格化できる．しばしば固有値 λ に対応する固有ベクトルを $|\lambda\rangle$ とかく．

$\{|e_k\rangle\}$ を正規直交基底とし，$\langle e_i|A|e_j\rangle = A_{ij}$, $|v\rangle = \sum_k v_k|e_k\rangle$ とすると固有値方程式の成分表示は

$$\sum_j A_{ij}v_j = \lambda v_i \tag{18}$$

となる．次に固有値を求めよう．固有値方程式 $\sum_j (A-\lambda I)_{ij}v_j = 0$ は係数の行列式がゼロとなるときのみ自明でない解 $\{v_j\}$ をもつ．すなわち

$$D(\lambda) \equiv \det(A-\lambda I) = 0 \tag{19}$$

$A \in M(n,\mathbb{C})$ の固有値を $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ とかくと $D(\lambda)$ は

$$\begin{aligned} D(\lambda) &= \prod_{i=1}^{n}(\lambda_i - \lambda) \\ &= (-\lambda)^n + \sum_i \lambda_i(-\lambda)^{(n-1)} + \ldots + \prod_{i=1}^{n}\lambda_i \\ &= (-\lambda)^n + \mathrm{tr}\,A(-\lambda)^{(n-1)} + \ldots + \det A, \end{aligned} \tag{20}$$

となる．ここで $\mathrm{tr}\,A = \sum_i \lambda_i$ および $\det A = \prod_i \lambda_i$ を用いた．

定理 2.1 エルミート行列の固有値はすべて実数である．また，相異なる固有値に属する固有ベクトルは直交する．

証明：A はエルミート行列で $A|v\rangle = \lambda|v\rangle$ とする．エルミート共役をとると $\langle v|A = \lambda^*\langle v|$．前者に左から $\langle v|$ を，後者に右から $|v\rangle$ をかけると $\langle v|A|v\rangle = \lambda\langle v|v\rangle = \lambda^*\langle v|v\rangle$, となり $\lambda = \lambda^*$ が得られる．次に $A|u\rangle = \mu|u\rangle$ $(\mu \neq \lambda)$ とする．$\mu \in \mathbb{R}$ から $\langle u|A = \mu\langle u|$ である．したがって $\langle u|A|v\rangle = \lambda\langle u|v\rangle$ と $\langle u|A|v\rangle = \mu\langle u|v\rangle$ から $0 = (\lambda-\mu)\langle u|v\rangle$ が得られる．$\mu \neq \lambda$ から $\langle u|v\rangle = 0$ となる． ∎

λ が k 重に縮退しているとすると，λ に対応する k 個の線型独立な固有ベクトルが存在する．これらから Gram-Schmidt の方法で k 次元の正規直交系をつくることができる．しがたって，エルミート行列の固有ベクトルは一般性を失うことなしに正規直交基底にとることができる．したがってエルミート行列 A の規格化された固有ベクトル $\{|e_k\rangle\}$ は完全系となる：

$$\sum_{k=1}^{n} |e_k\rangle\langle e_k| = I_n$$

例 2.3 Pauli 行列

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

はエルミートである．固有値方程式 $\det(\sigma_y - \lambda I) = \lambda^2 - 1 = 0$, から，固有値 $\lambda_1 = 1$ と $\lambda_2 = -1$. 固有ベクトルは

$$\sigma_y|\lambda_1\rangle = |\lambda_1\rangle,\ \sigma_y|\lambda_2\rangle = -|\lambda_2\rangle$$

を満たす．したがって，規格化された固有ベクトルは

$$|\lambda_1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \quad |\lambda_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} i \\ 1 \end{pmatrix}$$

これらが正規直交系で，完全性関係を満たすことは各自確かめよ．

最後に σ_y を対角化するユニタリー行列

$$U^\dagger \sigma_y U = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

を求めよう．直ちに分かるように

$$U = (|\lambda_1\rangle, |\lambda_2\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} i & 1 \\ 1 & i \end{pmatrix}$$

とおくと $AU = (A|\lambda_1\rangle, A|\lambda_2\rangle) = (\lambda_1|\lambda_1\rangle, \lambda_2|\lambda_2\rangle)$, であるから

$$U^\dagger A U = \begin{pmatrix} \langle\lambda_1| \\ \langle\lambda_2| \end{pmatrix} (\lambda_1|\lambda_1\rangle, \lambda_2|\lambda_2\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

となる．U がユニタリーであることは $\{|\lambda_k\rangle\}$ の正規直交性に基づく．

問 2.5 (1) A は反エルミート，すなわち $A^\dagger = -A$ であるとする．A の固有値はすべて純虚数であることを示せ．

(2) U はユニタリー行列とする．U のすべての固有値の絶対値は 1 であることを示せ

問 2.6 H はエルミート行列とする．このとき H の Cayley 変換

$$U = (I + iH)(I - iH)^{-1} \tag{21}$$

はユニタリーであることを示せ．

2.5　スペクトル分解

エルミート行列のスペクトル分解は，様々な応用をもち重要である．

定理 2.2 A をエルミート行列とし，その固有値，固有ベクトルを $\{\lambda_i\}, \{|\lambda_i\rangle\}$ とする．$\{|\lambda_i\rangle\}$ は正規直交系となるようにとると A は

$$A = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|, \tag{22}$$

と分解される（**スペクトル分解**）.

証明: 2つの行列 A と B が任意のベクトルに作用したときに同じベクトルを与えれば A と B は等しい. $\{|\lambda_i\rangle\}$ は正規直交基底であるから，任意のベクトルは $|v\rangle = \sum_i v_i|\lambda_i\rangle$ と分解される. A を $|v\rangle$ に作用させると $A|v\rangle = \sum_i v_i A|\lambda_i\rangle = \sum v_i\lambda_i|\lambda_i\rangle$ となる. 一方

$$\left[\sum_k \lambda_k|\lambda_k\rangle\langle\lambda_k|\right]\sum_i v_i|\lambda_i\rangle = \sum_{i,k} v_i\lambda_k|\lambda_k\rangle\langle\lambda_k|\lambda_i\rangle = \sum_{i,k} v_i\lambda_k|\lambda_k\rangle\delta_{ik} = \sum_i v_i\lambda_i|\lambda_i\rangle$$

である. $|v\rangle$ は任意であるから定理が証明された. ∎

例 2.4 例2.3を用いると σ_y のスペクトル分解は

$$A = \sum_i \lambda_i|\lambda_i\rangle\langle\lambda_i| = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} + (-1)\frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$$

で与えられる.

スペクトル分解の利点の一つは，行列の関数が容易に求められることである.

命題 2.1 A をエルミート行列とすると，任意の $n \in \mathbf{N}$ にたいし

$$A^n = \sum_i \lambda_i^n|\lambda_i\rangle\langle\lambda_i| \tag{23}$$

が成り立つ. さらに A^{-1} が存在すれば，この公式は $n \in \mathbf{Z}$ に拡張される.

証明: 数学的帰納法で証明しよう. $n = 1$ は自明である. $A^k|\lambda_i\rangle = \lambda_i^k|\lambda_i\rangle = \lambda_i^k|\lambda_i\rangle$ が $n = k \geq 2$ にたいし成り立つとすると $A^{k+1}|\lambda_i\rangle = \lambda_i^k A|\lambda_i\rangle = \lambda_i^{k+1}|\lambda_i\rangle$. したがって，$A^n$ は任意の $n \geq 1$ にたいし固有値 λ_i^n，対応する固有ベクトル $|\lambda_i\rangle$ をもつ. したがって (23) は任意の $n \in \mathbf{N}$ で成立.

A^{-1} が存在するとき A^{-1} は固有値 λ_i^{-1} と固有ベクトル $|\lambda_i\rangle$ をもつ. 実際 $A|\lambda_i\rangle = \lambda_i|\lambda_i\rangle \to |\lambda_i\rangle = \lambda_i A^{-1}|\lambda_i\rangle \to A^{-1}|\lambda_i\rangle = \lambda_i^{-1}|\lambda_i\rangle$ が成り立つ. 以下は前半と同様に証明される. ∎

これから一般にエルミート行列 A の任意の解析関数 $f(A)$ に対し

$$f(A) = \sum_i f(\lambda_i)|\lambda_i\rangle\langle\lambda_i|$$

が成り立つ.

命題 2.2 $\boldsymbol{n}$ を3次元実単位ベクトルとする. このとき

$$e^{i\alpha\boldsymbol{n}\cdot\boldsymbol{\sigma}} = \cos\alpha\, I_2 + i(\boldsymbol{n}\cdot\boldsymbol{\sigma})\sin\alpha. \tag{24}$$

証明 まず $\sigma_{\boldsymbol{n}} \equiv \boldsymbol{n}\cdot\boldsymbol{\sigma}$ のスペクトル分解を行う. 固有値と規格化された固有ベクトルは

$$\lambda_1 = +1,\ |\lambda_1\rangle = \sqrt{\frac{1-n_z}{2}}\begin{pmatrix} \sqrt{\dfrac{1+n_z}{n_x+in_y}} \\ 1 \end{pmatrix};\ \lambda_2 = -1,\ |\lambda_2\rangle = \sqrt{\frac{1+n_z}{2}}\begin{pmatrix} -\sqrt{\dfrac{1-n_z}{n_x+in_y}} \\ 1 \end{pmatrix}$$

したがって

$$\begin{aligned} e^{i\alpha \boldsymbol{n}\cdot\boldsymbol{\sigma}} &= e^{i\alpha}|\lambda_1\rangle\langle\lambda_1| + e^{-i\alpha}|\lambda_2\rangle\langle\lambda_2| \\ &= \frac{e^{i\alpha}}{2}\begin{pmatrix} 1-n_z & n_x-in_y \\ n_x+in_y & 1+n_z \end{pmatrix} + \frac{e^{-i\alpha}}{2}\begin{pmatrix} 1+n_z & -n_x+in_y \\ -n_x-in_y & 1-n_z \end{pmatrix} \\ &= \cos\alpha\, I_2 + i(\boldsymbol{n}\cdot\boldsymbol{\sigma})\sin\alpha. \end{aligned}$$

∎

問 2.7 2×2 のエルミート行列 A が固有値 $-1, 3$ と，対応する固有ベクトル

$$|e_1\rangle = \begin{pmatrix} -1 \\ i \end{pmatrix}, |e_2\rangle = \begin{pmatrix} 1 \\ i \end{pmatrix}$$

をもっているとする．A を求めよ．(注意：これらの固有ベクトルは規格化されていない.)

2.6　パウリ行列

スピン 1/2 の粒子は内部自由度 (spin-up (↑), spin-down (↓)) をもっている．これらの状態を

$$|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{25}$$

で表すことにしよう．($\sigma_z|\uparrow\rangle = |\uparrow\rangle$, $\sigma_z|\downarrow\rangle = -|\downarrow\rangle$ を確かめよ．) 量子情報では $|0\rangle = |\uparrow\rangle$ および $|1\rangle = |\downarrow\rangle$ と表すことが多い．一般に $|0\rangle$ と $|1\rangle$ は必ずしもスピンを表すとは限らない．これらは２つの直交する状態であれば何でもよい．以下スピン代数をしばしば用いるが $|0\rangle, |1\rangle$ が何を意味するかは考えている物理系によるのである．

パウリスピン行列 σ_k は $\mathfrak{su}(2)$ 代数の生成子で

$$\mathrm{tr}\,\sigma_k = 0, \qquad \sigma_k^\dagger = \sigma_k \tag{26}$$

を満たす．$I = \sigma_0$ と定義することもある．I を含めることにより $\mathfrak{su}(2)$ 代数は $\mathfrak{u}(2)$ に拡張される．反交換関係

$$\{\sigma_i, \sigma_j\} = \sigma_i\sigma_j + \sigma_j\sigma_i = 2\delta_{ij}I \tag{27}$$

を確かめよ．これから σ_k の固有値が ± 1 であることが示される．

パウリ行列の交換関係は

$$[\sigma_i, \sigma_j] = \sigma_i\sigma_j - \sigma_j\sigma_i = 2i\sum_k \varepsilon_{ijk}\sigma_k \tag{28}$$

である．この２つの (反) 交換関係から

$$\sigma_i\sigma_j = i\sum_{k=1}^{3}\varepsilon_{ijk}\sigma_k + \delta_{ij}, \tag{29}$$

が得られる．ここに ε_{ijk} は3階の完全反対称テンソル（Levi-Civita シンボル）である．[4]

スピン反転演算子を

$$\sigma_+ = \frac{1}{2}(\sigma_x + i\sigma_y) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \sigma_- = \frac{1}{2}(\sigma_x - i\sigma_y) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \tag{30}$$

で定義すると $\sigma_+|\uparrow\rangle = \sigma_-|\downarrow\rangle = 0$, $\sigma_+|\downarrow\rangle = |\uparrow\rangle$, $\sigma_-|\uparrow\rangle = |\downarrow\rangle$ が示される．$\sigma_z = \pm 1$ の固有状態への射影演算子は

$$\Lambda_+ = |\uparrow\rangle\langle\uparrow| = \frac{1}{2}(I + \sigma_z) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \Lambda_- = |\downarrow\rangle\langle\downarrow| = \frac{1}{2}(I - \sigma_z) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{31}$$

で与えられる．実際 $\Lambda_+|\uparrow\rangle = |\uparrow\rangle$, $\Lambda_+|\downarrow\rangle = 0$, $\Lambda_-|\uparrow\rangle = 0$, $\Lambda_-|\downarrow\rangle = |\downarrow\rangle$ が満たされる．

問 2.8 $f : \mathbb{C} \to \mathbb{C}$ を関数とし，$\hat{\boldsymbol{n}} \in \mathbb{R}^3$ を単位ベクトル，α を実数とする．このとき

$$f(\alpha \hat{\boldsymbol{n}} \cdot \boldsymbol{\sigma}) = \frac{f(\alpha) + f(-\alpha)}{2} I + \frac{f(\alpha) - f(-\alpha)}{2} \hat{\boldsymbol{n}} \cdot \boldsymbol{\sigma}. \tag{32}$$

を示せ．これは命題2.2の一般化である．

2.7 テンソル積

以下で多粒子系の演算子や状態を表すのテンソル積が使われる．通常，Ising モデルなどで2個のスピンの積を $\sigma_z\sigma_z$ と書くが，数学的にはこれは通常の行列の積とは異なり，テンソル積 $\sigma_z \otimes \sigma_z$ を表す．

定義 2.4 A を $m \times n$ 行列，B を $p \times q$ 行列とすると

$$A \otimes B = \begin{pmatrix} a_{11}B, a_{12}B, \ldots, a_{1n}B \\ a_{21}B, a_{22}B, \ldots, a_{2n}B \\ \cdots \\ a_{m1}B, a_{m2}B, \ldots, a_{mn}B \end{pmatrix} \tag{33}$$

は $(mp) \times (nq)$ 行列となる．これを A と B の**テンソル積**という．

すべての $(mp) \times (nq)$ 行列がテンソル積でかけるとは限らないことに注意せよ．$A \otimes B$ は $mn + pq$ の独立成分しか持たないが，一般の $(mp) \times (nq)$ 行列は，はるかに多い $mnpq$ 成分を持つ．

例 2.5

$$\sigma_x \otimes \sigma_z = \begin{pmatrix} 0 & \sigma_z \\ \sigma_z & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

[4] $\varepsilon_{ijk} = \begin{cases} 1, & (ijk) = (123), (312), (231) \\ -1, & (ijk) = (213), (321), (132) \\ 0, & \text{その他} \end{cases}$

ベクトルも行列の特別な場合と考えるとテンソル積が定義される.

$$|u\rangle = \begin{pmatrix} a \\ b \end{pmatrix},\ |v\rangle = \begin{pmatrix} c \\ d \end{pmatrix} \Rightarrow |u\rangle \otimes |v\rangle = \begin{pmatrix} a|v\rangle \\ b|v\rangle \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

問 2.9 A, B は定義2.4のようであるとし，C を $n \times r$ 行列，D を $q \times s$ 行列とする．このとき

$$(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD) \tag{34}$$

を示せ．ただし左辺の積 $\cdot$ は通常の行列の積である.

したがって

$$(A \otimes B)(|u\rangle \otimes |v\rangle) = (A|u\rangle) \otimes (B|v\rangle) \tag{35}$$

が成り立つ．同様に各行列の次数がマッチして積がうまく定義されれば

$$(A_1 \otimes B_1) \cdot (A_2 \otimes B_2) \cdot (A_3 \otimes B_3) = (A_1 A_2 A_3) \otimes (B_1 B_2 B_3)$$

などが成り立つ.

問 2.10 (1)

$$A \otimes (B + C) = A \otimes B + A \otimes C \tag{36}$$

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger \tag{37}$$

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1} \tag{38}$$

を示せ．ただし積は定義できているものとする.
(2) A, B はそれぞれ $m \times m$ 行列と $p \times p$ 行列とする．このとき

$$\mathrm{tr}\,(A \otimes B) = (\mathrm{tr}\,A)(\mathrm{tr}\,B) \tag{39}$$

$$\det(A \otimes B) = (\det A)^p (\det B)^m \tag{40}$$

を示せ.

問 2.11 (1) ユニタリー行列のテンソル積はユニタリーであることを示せ.
(2) エルミート行列のテンソル積はエルミートであることを示せ.

問 2.12 (1) $|a\rangle, |b\rangle, |c\rangle, |d\rangle \in \mathbb{C}^n$ のとき $(|a\rangle\langle b|) \otimes (|c\rangle\langle d|) = (|a\rangle \otimes |c\rangle)(\langle b| \otimes \langle d|)$ を示せ.
(2) $P_i = |i\rangle\langle i|$ と $P_j = |j\rangle\langle j|$ は射影演算子とする．このとき $P_i \otimes P_j = |ij\rangle\langle ij|$ を示せ．ただし $|ij\rangle = |i\rangle \otimes |j\rangle$.

定理 2.3 A は $m \times m$ 行列，B は $p \times p$ 行列とする．A の固有値，固有ベクトルを $\lambda_1, \ldots, \lambda_m$, $|u_1\rangle, \ldots, |u_m\rangle$，$B$ の固有値，固有ベクトルを $\mu_1, \ldots, \mu_p$, $|v_1\rangle, \ldots, |v_p\rangle$ とする．このとき $A \otimes B$ は mp 個の固有値 $\{\lambda_j \mu_k\}$ と対応する固有ベクトル $\{|u_j\rangle \otimes |v_k\rangle\}$ をもつ．

証明: $|u_j\rangle \otimes |v_k\rangle$ が固有ベクトルであることを示す．実際

$$\begin{aligned}(A \otimes B)(|u_j\rangle \otimes |v_k\rangle) &= (A|u_j\rangle) \otimes (B|v_k\rangle) = (\lambda_j |u_j\rangle) \otimes (\mu_k |v_k\rangle) \\ &= \lambda_j \mu_k (|u_j\rangle \otimes |v_k\rangle)\end{aligned}$$

したがって，その固有値は $\lambda_j \mu_k$ で対応する固有ベクトルは $|u_j\rangle \otimes |v_k\rangle$ となる．mp 個の固有値があるので，これはすべての固有値を尽くしている． ∎

問 2.13 A, B は上の定理に与えられた行列とする．このとき $A \otimes I_p + I_m \otimes B$ は固有値 $\{\lambda_j + \mu_k\}$ と，対応する固有ベクトル $\{|u_j\rangle \otimes |v_k\rangle\}$ をもつことを示せ．

3 量子力学の枠組み

読者の多くは量子力学に習熟しているものと思われるので，本節では以下の解説に必要最低限の事実と例を述べるに留める．量子力学はいくつかの公理から成り立っている．公理の選び方は人にまた目的に依存するが，ここでは量子情報をあつかうのにもっとも適当な公理を紹介する．

3.1 量子力学の公理

A 1 量子力学の純粋状態は，あるヒルベルト空間の単位ベクトル $|\psi\rangle$ で表される．ベクトルの位相は勝手にとってもよい：$|\psi\rangle$ と $e^{i\alpha}|\psi\rangle$ は同一状態を表す．

A 2 2つの状態 $|\psi\rangle$ と $|\phi\rangle$ が物理的に実現可能な状態とする．するとそれらの線型結合 $a|\psi\rangle + b|\phi\rangle$ $(a, b \in \mathbb{C})$ も同じ系の物理的に実現可能な状態である．これを**重ね合わせの原理**という．$|\psi\rangle$ の位相は意味をもたないが2つの状態の相対位相は意味をもつ．すなわち $|\psi_1 + \psi_2\rangle$ と $|\psi_1 + e^{i\alpha}\psi_2\rangle$ は異なる状態を表す．

A 3 量子状態の時間発展は**シュレーディンガー方程式**

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = H|\psi\rangle \tag{41}$$

に従う．これは形式的に解かれ，H が時間に依存しなければ解は

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle \tag{42}$$

となり，時間に依存すれば

$$|\psi(t)\rangle = \mathcal{T} \exp\left[-\frac{i}{\hbar}\int_0^t H(t)dt\right]|\psi(0)\rangle \tag{43}$$

で与えられる．$\mathcal{T}$ は**時間順序積演算子**である．[5]演算子 $U:|\psi(0)\rangle \mapsto |\psi(t)\rangle$ はユニタリーなので $|\psi(t)\rangle$ のノルムは保存する：$\langle\psi(0)|U^\dagger U|\psi(0)\rangle = \langle\psi(0)|\psi(0)\rangle$ $(=1)$.

A 4 任意の物理量 a にたいし，それに対応するヒルベルト空間上のエルミート演算子 A が存在する．a を測定したとき得られる値は A の固有値 $\{a_j\}$ の一つである．a_1, a_2 を A の 2 つの固有値とする．系が重ね合わせ状態 $c_1|a_1\rangle + c_2|a_2\rangle$ にあるとき a を測定すると系は測定値に応じて $|a_i\rangle$ のどちらかに遷移する：a_1 (a_2) が観測されれば，系は $c_1|a_1\rangle + c_2|a_2\rangle \to |a_1\rangle$ $(|a_2\rangle)$ と「波束の収縮」を行う．$|a_k\rangle$ に遷移する確率は $|c_k|^2$ $(k=1,2)$ で与えられる．観測による状態変化 $c_1|a_1\rangle + c_2|a_2\rangle \to |a_k\rangle$ は逆をもたないので，観測過程はユニタリーではない．

A 5 N 個の部分からなる系を考える．それぞれのヒルベルト空間を $\mathcal{H}_k$ とすると，全系のヒルベルト空間はそのテンソル積 $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_N$ で与えられる．

3.2　いくつかの例

前章で学んだ線型代数を量子力学のいくつかの問題に応用しよう．これらは量子計算の物理系における実装に応用される．

例 3.1 (1) ハミルトニアン $H = \hbar\omega\sigma_z/2$ を考える．初期状態を $|\psi(0)\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ とすると，波動関数 $|\psi(t)\rangle$ は

$$|\psi(t)\rangle = \exp\left[-\frac{i}{\hbar}Ht\right]|\psi(0)\rangle = \begin{pmatrix} \exp(-i\omega t/2) & 0 \\ 0 & \exp(i\omega t/2) \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \exp(-i\omega t/2) \\ 0 \end{pmatrix} \tag{44}$$

となる．これは初期状態が H の固有ベクトルであることから明らかである．系がこの固有状態にある確率は，任意の t において $|\exp(-i\omega t/2)|^2 = 1$

(2) ハミルトニアンを $H = \hbar\omega\sigma_x/2$ とする．系の初期状態を $|\psi(0)\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ とする．命題 2.2 を用いて

$$\begin{aligned} |\psi(t)\rangle &= e^{-i\omega\sigma_x t/2}|\psi(0)\rangle = (\cos\omega t/2 I - i\sigma_x \sin\omega t/2)|\psi(0)\rangle \\ &= \begin{pmatrix} \cos\omega t/2 & -i\sin\omega t/2 \\ -i\sin\omega t/2 & \cos\omega t/2 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\omega t/2 \\ -i\sin\omega t/2 \end{pmatrix} \end{aligned} \tag{45}$$

が得られる．時刻 t においてこのスピンを観測したとき $\sigma_z = +1$ が得られる確率は $|\cos\omega t/2|^2 = \cos^2\omega t/2$ で与えられ，$\sigma_3 = -1$ が得られる確率は $|-i\sin\omega t/2|^2 = \sin^2\omega t/2$ で与えられる．その和が 1 であることは言うまでもない．

---

[5] 2 つの時間 t に依存する演算子 $A(t)$, $B(t)$ に関し

$$\mathcal{T}[A(t_1)B(t_2)] = \begin{cases} A(t_1)B(t_2) & t_1 > t_2 \\ B(t_2)A(t_1) & t_2 \geq t_1 \end{cases}$$

一般化は容易であろう．

問 3.1 ハミルトニアン

$$H = \hbar\omega\sigma_y/2 = \frac{\hbar\omega}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{46}$$

を考える．系は初期状態 $|\psi(0)\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ にあったとする．

(1) 時刻 $t > 0$ における波動関数 $|\psi(t)\rangle$ を求めよ．

(2) $t > 0$ において系が固有値 $\sigma_z = +1$ を持つ確率をもとめよ．

(3) $t > 0$ において系が $\sigma_x = +1$ をもつ確率を求めよ．

例 3.2 (Rabi 振動) この例は量子計算の実現において特に重要である．ハミルトニアン

$$H_0 = \begin{pmatrix} 0 & 0 \\ 0 & \hbar\epsilon \end{pmatrix} \qquad (\epsilon > 0) \tag{47}$$

を考える．系の初期状態を $|\psi(0)\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ とする．$0 \leq t \leq T$ の間，この系に振動数 ω のコヒーレントな電磁波を照射すると，摂動を受けたハミルトニアンは

$$H = \begin{pmatrix} 0 & \mu e^{i\omega t} \\ \mu e^{-i\omega t} & \hbar\epsilon \end{pmatrix} \tag{48}$$

で与えられる．非対角要素は光子の吸収，放出を表している．この系の波動関数を

$$|\psi(t)\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{49}$$

とかく．計算の便宜上 $\alpha = a$ および $\beta = e^{-i\omega t}b$ とおくと Schrödinger 方程式は

$$i\hbar\frac{\partial}{\partial t}\begin{pmatrix} a \\ b \end{pmatrix} = \tilde{H}\begin{pmatrix} a \\ b \end{pmatrix} \tag{50}$$

となる．ここに

$$\tilde{H} = \begin{pmatrix} 0 & \mu \\ \mu & \hbar(\epsilon - \omega) \end{pmatrix} \tag{51}$$

は t によらないことに注意しよう．$\tilde{H}$ は固有値

$$\lambda_\pm = \frac{\hbar(\epsilon - \omega) \pm \sqrt{\hbar^2(\epsilon - \omega)^2 + 4\mu^2}}{2} \tag{52}$$

と，対応する規格化された固有ベクトル

$$|\lambda_\pm\rangle = \frac{1}{\sqrt{\lambda_\pm^2 + \mu^2}}\begin{pmatrix} \mu \\ \lambda_\pm \end{pmatrix} \tag{53}$$

をもつ．これからシュレーディンガー方程式の解は

$$|\phi(t)\rangle = C_+ e^{-i\lambda_+ t}|\lambda_+\rangle + C_- e^{-i\lambda_- t}|\lambda_-\rangle \tag{54}$$

で与えられることがわかる．系は$t=0$で基底状態にあったので，初期条件は

$$|\phi(0)\rangle = |\psi(0)\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{55}$$

である．$t>0$における波動関数はこの初期条件を代入して$C_\pm$を求めれば得られる．結果は

$$C_+ = \frac{\mu}{\sqrt{\lambda_+^2+\mu^2}}, C_- = \frac{\mu}{\sqrt{\lambda_-^2+\mu^2}}$$

から

$$|\phi(t)\rangle = \frac{\mu e^{-i\lambda_+ t}}{\lambda_+^2+\mu^2}\begin{pmatrix} \mu \\ \lambda_+ \end{pmatrix} + \frac{\mu e^{-i\lambda_- t}}{\lambda_-^2+\mu^2}\begin{pmatrix} \mu \\ \lambda_- \end{pmatrix}. \tag{56}$$

特に，電磁波が2準位のエネルギー差と共鳴する場合を考える：$\omega=\epsilon$．このとき$\lambda_\pm \to \pm\mu$となり，$t>0$における波動関数は

$$|\phi(t)\rangle = \begin{pmatrix} \cos\mu t \\ -i\sin\mu t \end{pmatrix} \tag{57}$$

と簡単になる．これからHの波動関数は

$$|\psi(t)\rangle = \begin{pmatrix} \cos\mu t \\ -ie^{-i\omega t}\sin\mu t \end{pmatrix} \tag{58}$$

と求められる．したがって系が基底状態（励起状態）にある確率は$P_0=\cos^2\mu t$　$(P_1=\sin^2\mu t)$で与えられる．この振動の様子はRabi振動と呼ばれる．

4　量子ビットと簡単な応用

量子系で2つの固有状態をもつものを考える．これは(1) 原子の2準位 (2) スピン1/2の粒子のスピン状態 (3) 光子の偏光状態，などが挙げられる．以下では物理系にかかわらず，2状態を

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

で表す．

4.1　量子ビット

4.1.1　1量子ビット

古典情報理論は0と1の値をとるビットに基づく．一方，量子情報理論は「**量子ビット** (quantum bit = **qubit**)」を単位とする．量子ビットは$\mathbb{C}^2$の（単位）ベクトルである．その基底を$\{|0\rangle,|1\rangle\}$とかく．それぞれの基底ベクトルがどんな物理状態を表すかは，上に述べたように用いるリソースに依存する．

量子計算ではベクトル $|0\rangle$ は古典的な 0 に，$|1\rangle$ は 1 に対応するとしてもよい．しかし古典ビットとの大きな違いは，量子ビットは重ね合わせ状態

$$a|0\rangle + b|1\rangle, \qquad |a|^2 + |b|^2 = 1 \tag{59}$$

をとることができるという点である．量子力学の公理により，この状態が $|0\rangle$ か $|1\rangle$ かを観測すると，確率 $|a|^2$ で $|0\rangle$ が，$|b|^2$ で $|1\rangle$ が観測される．

したがって，量子ビットは無限の状態を取りうるものの，それから得られる情報は古典ビットと同じく 0 か 1 である．情報は観測によってのみ得る事ができ，その結果量子ビットの状態は観測された状態に「収縮」してしまう．したがって，量子ビットが $|0\rangle$ にあることが観測されると，その直後の状態は確率 1 で $|0\rangle$ である．前節で述べたように観測のプロセスはユニタリーではないので，観測結果から観測前の量子ビットの状態を知ることはできない．与えられた量子ビットのコピーを沢山用意して同じ測定を何度も繰り返せば，少なくとも $|a|, |b|$ は分かりそうに思われるが，以下に証明する「No-Cloning 定理」により，未知の状態をコピーすることは不可能なので，それもできない．

この事実は量子アルゴリズムをデザインするうえで重要なポイントとなる．結果が確率的なので，答えの正当性を確かめがたい計算には不向きである．ところが結果の正当性を確かめるのが容易な問題，たとえば素因数分解やデータベース検索などは量子計算が得意とする分野である．また量子アルゴリズムは，望む結果を与える確率が増幅され，それ以外の確率が減少するようにデザインしなければならない．

4.1.2 n 量子ビットともつれた状態 (Entangled state)

次に複数の量子ビットからなる系を考えよう．このような系は古典的直感と全く異なるふるまいをし，それが量子情報に大きなパワーを与える．いくつかの部分からなる古典系が与えられると，全系の状態は各部分系の状態を指定すれば一意的に決まる．しかし量子系はこのように部分系に分けて考えられるとは限らない．例えば，各部分系が 2 自由度をもっているとしよう．古典的には n 個のこのような系は $2n$ の自由度をもつ．一方量子系ではそのヒルベルト空間は $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$ となり，自由度は 2^n となるのである．

まず 2 量子ビット系を考えよう．各量子ビットは基底 $\{|0\rangle, |1\rangle\}$ をもつので，全系の基底は $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$ で与えられる．これをコンパクトに $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ と書く事もある．また 10 進法で $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ とも書く．一般に n 量子ビット系の基底は $\{|b_{n-1}b_{n-2}\ldots b_0\rangle\}$, $b_{n-1}, b_{n-2}, \ldots, b_0 \in \{0, 1\}$ で与えられる．10 進法で $x = b_{n-1}2^{n-1} + b_{n-2}2^{n-2} + \ldots + b_0$ のとき，$|b_{n-1}b_{n-2}\ldots b_0\rangle$ の代わりに $|x\rangle$ と書くこともある．このように n 量子ビット系は 2^n 個の基底ベクトルを持つ．この指数関数的な基底ベクトルの増加も量子計算の大きなパワーとなる．

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ は 2 つの量子状態のテンソル積ではかけない状態の例である．実際

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) \quad = \quad a_1a_2|00\rangle + a_1b_2|01\rangle + a_2b_1|10\rangle + a_2b_2|11\rangle$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

と書けたとすると，係数 a_i, b_i は $a_1 b_2 = 0 \to a_1 a_2 = 0$ または $a_2 b_2 = 0$ を満たさなければならないが，これは矛盾．テンソル積で表せない状態を**もつれた状態 (entangled state)** という．もつれた状態は古典的アナロジーを持たず，量子情報処理で主要な役割を果たす．古典的記述を許すもつれていない状態は

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) \otimes (a_n|0\rangle + b_n|1\rangle)$$

と $2n$ 個のパラメタをもつ．これは 2^n 次元のヒルベルト空間の限られた部分集合である．ヒルベルト空間の大部分の元は古典的なアナロジーを持たない量子系に特有の状態である．

問 4.1 以下の状態の中でもつれた状態はどれか？テンソル積でかける状態は，それをテンソル積で表せ．

$$(1)\ \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\quad (2)\ \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)\quad (3)\ \frac{1}{\sqrt{2}}(|101\rangle + |111\rangle)$$
$$(4)\ \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)\quad (5)\ \frac{1}{2}(|000\rangle + |001\rangle + |100\rangle + |101\rangle).$$

4.1.3　測定

古典情報理論は系の測定とは独立に定式化されているが，これは系が同じ情報を処理している限り，その出力は誰がいつ測定しても常に同じ結果となるからである．一方，量子情報では以下に示すように測定は情報処理の主要な部分である．

量子系を測定すると，系は測定器が定義する基底ベクトルのひとつに射影される．[6]たとえば $|\psi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$ においてスピンの z 成分を測定するとしよう．その結果は↑か↓のどちらかである．最初の場合は波動関数は $|\uparrow\rangle$ に収縮し，後の場合は $|\downarrow\rangle$ に収縮する．どちらの結果が得られるかは確率的で，測定は状態 $|\psi\rangle$ を $|\uparrow\rangle$ か $|\downarrow\rangle$ にそれぞれ確率 $|a|^2$ と $|b|^2$ で射影する．

より具体的には，測定演算子 M_m を導入する．$|\psi\rangle$ において観測結果 m を得る確率は

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{60}$$

で与えられ，測定直後の状態は

$$|m\rangle = \frac{M_m|\psi\rangle}{\sqrt{p(m)}} \tag{61}$$

となる．上の例では測定演算子は射影演算子に他ならない：$M_\uparrow = |\uparrow\rangle\langle\uparrow|, M_\downarrow = |\downarrow\rangle\langle\downarrow|$．実際 $p(\uparrow) = \langle\psi|M_\uparrow^\dagger M_\uparrow|\psi\rangle = \langle\psi|\uparrow\rangle\langle\uparrow|\psi\rangle = |a|^2$ および $\frac{M_\uparrow|\psi\rangle}{\sqrt{p(\uparrow)}} = \frac{a}{|a|}|\uparrow\rangle \simeq |\uparrow\rangle$ で，↓に関しても同様である．

[6]これは射影測定とよばれる．以下では射影測定しか扱わない．

測定演算子 M を同一の量子系 $|\psi\rangle$ にたいし，何度も測定すると M の期待値が得られる：

$$E(M) = \sum_m mp(m) = \sum_m m\langle\psi|P_m|\psi\rangle = \langle\psi|\sum_m mP_m|\psi\rangle = \langle\psi|M|\psi\rangle. \tag{62}$$

ここに M のスペクトル分解 $M = \sum_m mP_m$ を用いた．測定値の標準偏差は

$$\Delta(M) = \sqrt{\langle(M - \langle M\rangle)^2\rangle} = \sqrt{\langle M^2\rangle - \langle M\rangle^2} \tag{63}$$

で与えられる．

問 4.2 (不確定性関係)

(1) A と B をエルミート演算子とし $|\psi\rangle$ を A, B が作用する状態とする．このとき $|\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2$ を示せ．

(2) Cauchy-Schwarz 不等式 $|\langle\psi|AB|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$ を証明せよ．

(3) 不等式 $|\langle\psi|[A,B]|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$ を証明せよ．

(4) 不等式

$$\Delta(A)\Delta(B) \geq \frac{1}{2}|\langle\psi|[A,B]|\psi\rangle| \tag{64}$$

を証明せよ．

(5) $A = Q$ および $B = \dfrac{\hbar}{i}\dfrac{d}{dQ}$ とする．上の議論から $\Delta(Q)\Delta(P) \geq \dfrac{\hbar}{2}$ を証明せよ．

2 量子ビット系の測定を詳しく調べよう．任意の 2 量子ビット状態は

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad (a,b,c,d \in \mathbb{C},\ |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1)$$

とかかれる．1 番目の量子ビットを $\{|0\rangle, |1\rangle\}$ という基底で観測しよう．そこで状態を

$$\begin{aligned} a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle &= |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle) \\ &= u|0\rangle \otimes \left(\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle\right) + v|1\rangle \otimes \left(\frac{c}{v}|0\rangle + \frac{d}{v}|1\rangle\right) \end{aligned}$$

と書き直す．ここに $u = \sqrt{|a|^2 + |b|^2}$ および $v = \sqrt{|c|^2 + |d|^2}$ である．第 1 量子ビットに作用する測定演算子は $M_0 = |0\rangle\langle 0| \otimes I$ と $M_1 = |1\rangle\langle 1| \otimes I$ である．第 1 量子ビットを測定すると $\langle\psi|M_0|\psi\rangle = u^2 = |a|^2 + |b|^2$ の確率で 0 が得られ，状態は

$$\frac{M_0|\psi\rangle}{\sqrt{p(0)}} = |0\rangle \otimes \left(\frac{a}{u}|0\rangle + \frac{b}{u}|1\rangle\right)$$

へ射影される．また $\langle\psi|M_1|\psi\rangle = v^2 = |c|^2 + |d|^2$ の確率で 1 が得られ状態は $|1\rangle \otimes \left(\dfrac{c}{v}|0\rangle + \dfrac{d}{v}|1\rangle\right)$ へと射影される．測定後の状態もノルム 1 であることに注意せよ．第 2 量子ビットの観測も同様に行われる．(一般に n 量子ビット系の観測も 1 量子ビットの測定を繰り返して実行される．) 2 量子ビット系の場合，全系のヒルベルト空間は最初の量子ビットが $|0\rangle$ である $\mathcal{H}_0$ と $|1\rangle$ である $\mathcal{H}_1$ の直和でかかれる．任意の状態は一意的に $\mathcal{H}_{0,1}$ に属するベクトルの和で表される．より一般に n 量子ビット

中の k ビットを観測すると，その結果 m_i には 2^k 個の可能性がある：$1 \leq i \leq 2^k$．したがって 2^n 次元のヒルベルト空間は，互いに直交する 2^k 個の部分空間 $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_{2^k}$ の直和 $\mathcal{H} = \mathcal{H}_1 \oplus \ldots \oplus \mathcal{H}_{2^k}$ と表される．k 個の量子ビットの測定結果が m_i であるとき，観測直後の状態は $\mathcal{H}_i$ へ射影される．このように観測装置は観測前の状態 $|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle + \ldots + c_{2^k}|\psi_{2^k}\rangle$，$(|\psi_i\rangle \in \mathcal{H}_i)$ を部分空間 $\mathcal{H}_i$ の一つに確率 $|c_i|^2$ でランダムに射影する．

測定はもつれた状態に新たな視点を与える．もしある量子ビットの測定が他の量子ビットに何の影響も与えなければ，系はもつれた状態ではない．状態 $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ の第 1 量子ビットの測定が 0 (1) であったとしよう．すると第 2 量子ビットは確実に 0 (1) の状態にある．したがって第 1 量子ビットの測定は第 2 量子ビットの測定に影響を与え，最初の状態がもつれた状態であったことがわかる．一方，状態 $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ は $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ とかけるので，もつれた状態ではない．第 2 量子ビットの測定にかかわらず第 1 量子ビットは必ず 0 を与える．また第 2 量子ビットの測定において 0 (1) を得る確率は，第 1 量子ビットを観測するかどうかにかかわらず 1/2 である．

問 4.3 多くの量子アルゴリズムにおいて，関数 f の x に対する作用は

$$U_f : \sum_x |x\rangle|0\rangle \to \sum_x |x\rangle|f(x)\rangle,$$

という形で実現される．ここに $|x\rangle = |b_{n-1}b_{n-2}\ldots b_0\rangle$，ただし $x = b_{n-1}2^{n-1} + b_{n-2}2^{n-2} + \ldots + b_0$ である．即ち 1 番目のレジスターは入力を，2 番目のレジスターは出力を表す．ここで互いに素な自然数 m, N にたいし $f(x) = m^x \pmod N$ とおく．状態

$$U_f \frac{1}{\sqrt{512}} \sum_{x=0}^{511} |x\rangle|0\rangle = \frac{1}{\sqrt{512}} \sum_{x=0}^{511} |x\rangle|m^x \mathrm{mod} N\rangle$$

において $m = 6$ と $N = 91$ とおく．1 番目のレジスターの測定が (1) $x = 11$, (2) $x = 23$, (3) $x = 35$ であったとする．測定直後の状態を求めよ．

4.1.4 EPR (Einstein-Podolsky-Rosen) パラドックス

EPR はもつれた状態の存在は一見，特殊相対論の公理を破るとして以下の思考実験を提唱した．ある粒子源が **EPR 状態**

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

を発生したとする．それぞれの粒子は Alice と Bob へ送られる．Alice と Bob はとても離れているとしよう．Alice は彼女の粒子を測定し，結果が $|0\rangle$ $(|1\rangle)$ であったとする．すると EPR 状態は $|00\rangle$ $(|11\rangle)$ へ収縮し，Bob は彼の測定において確実に $|0\rangle$ $(|1\rangle)$ を観測する．状態の変化

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \;\to\; |00\rangle \quad \text{または} \quad |11\rangle \tag{65}$$

は彼らが如何に離れていても瞬時に発生する．したがって Alice は Bob に瞬時に「情報」を送ったように思われる．しかし Alice が測定結果を制御することは不可能であるので，Bob に意味があ

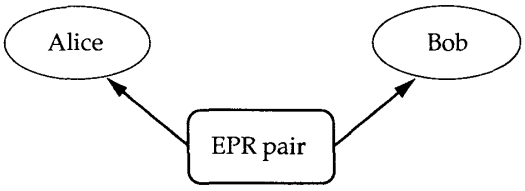


図 1: EPR ペア.

る情報を送ることはできない．パラドックスは，たんに 2 個の粒子の間に相関があるといっているだけである．

4.2 量子暗号鍵配布 (BB84 プルトコル)

ここでは 1 量子ビットの簡単な応用として，**量子暗号鍵配布 (QKD=Quantum Key Distribution)** を紹介する [7]. 暗号鍵の送信者も受信者も，彼らの通信を傍受している第 3 者が存在するかどうかを知ることができるので，これは非常に安全な鍵配布法であり，すでに商品化されている．

まず，暗号鍵について解説しよう．他人に鍵がもれない限り絶対安全な暗号として **one-time pad** がある．たとえばアルファベットでメッセージを送るとき，文字の順番ごとにそれをシフトさせる．例えば hello を 56321 とシフトすると暗号化されたメッセージ mkonp となる．(HAL を 111 とシフトすると IBM となるのはよく知られた例である．) 明らかに第 3 者が通信 mkonp を傍受しても，暗号鍵 56321 がなければ通信からもとのメッセージ hello を解読することは不可能である．傍受者があてずっぽうの数を暗号鍵として解読を試みても意味のあるメッセージは無数に現れるので，どれが正しいメッセージかは判別できない．しかし同じ暗号鍵を何度も用いると，やがてその規則性から暗号鍵を推測することができる．暗号鍵は使い捨てでただ 1 回，すなわち one-time pad として用いた時にのみ 100%安全な暗号となるのである．古典的には one-time pad の暗号鍵を配布する時の安全性が確かめられないので実用化はされなかったが，以下に述べる方法で量子ビットを用いると他者に除かれていないことが確証でき，one-time pad を安全に用いることができる．

Alice は Bob に暗号化されたメッセージを解く鍵を送りたいとする．彼らは古典的なチャネルを通して双方向通信でき，また Alice から Bob へ一方向の量子チャネルが存在するとしよう．かれらの通信は Eve によって傍受される可能性がある．Alice は Bob に沢山の量子ビットを 1 個ずつ送り，Bob はその状態を測定する．

Alice が例えば光子を量子ビットとして Bob に 1 個ずつ送るとき，Alice は 2 種類の偏光

$$(1)\quad 0 \mapsto |\updownarrow\rangle, 1 \mapsto |\leftrightarrow\rangle, \tag{66}$$

$$(2)\quad 0 \mapsto |\nwarrow\!\!\searrow\rangle, 1 \mapsto |\swarrow\!\!\nearrow\rangle \tag{67}$$

をランダムに用いるとする．Bob もそれぞれの光子を測定するのに，2 種類の偏光を Alice とは独

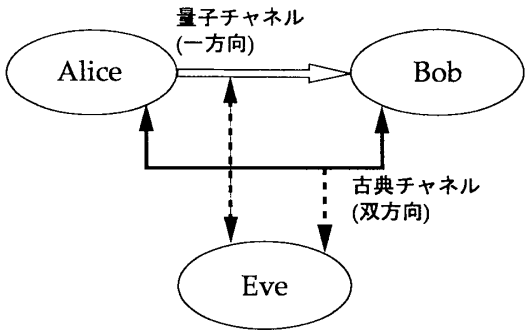


図 2: 量子暗号鍵配布プロトコル BB84.

立にやはりランダムに選ぶ．すべての光子が送られた後，Alice は Bob に古典チャネルを通して各光子ごとの偏光の方法 (1), (2) を伝えるが，各光子のデータが 0 か 1 であるかは秘密にしておく．その結果，同じ偏光を使ったのはどの光子かが分かり，それらの信号は Alice と Bob で一致しているはずである．彼らはそれ以外のすべてのデータを破棄し，同じ偏光を用いた光子の結果のみを保存し，それを暗号鍵として用いる．だれも傍受していなければ，約 50 %の偏光は一致しているはずである．長さ N ビットの暗号鍵が必要であれば平均して $2N$ の光子を送れば暗号鍵が生成できる．

次に傍受者 Eve が量子チャネルを覗いているとしよう．Eve も偏光 (1), (2) を用いて観測した結果をそのまま Bob に同じ偏光で送るとする．Eve の偏光は確率 1/2 で Alice のものと異なり，そのとき Eve は Bob に間違った偏光を用いて彼女の測定結果を送る．すると，Alice と Bob が同じ偏光を用いて光子を送受信したにもかかわらず，二人の測定結果が一致しないケースが出てくる．これは以下に示すように確率 1/4 で生じる：Alice も Bob も偏光 (1) を用いて 0 を送受したとしよう．Eve は確率 1/2 で (1) の偏光を採用し，そのときは必ず 0 を測定し，Bob に 0 を送るので Bob は確率 1 で 0 を測定する．一方，Eve は確率 1/2 で偏光 (2) を採用するが，このとき Eve が 0 (1) を測定する確率はそれぞれ 1/2 であり，その結果を偏光 (2) で Bob に送る．Bob は偏光 (1) を採用しているので 0 (1) を測定する確率は 1/2 である．結局，Bob はこの光子に関しては，Alice と同じ偏光を用いているのに確率 3/4 で 0，1/4 で 1 を測定することになる．したがって Alice が非常に多くの光子を送れば誰かが通信を傍受していることが分かるのである．

したがって，光子の送受信の最後に Alice と Bob は受信した信号の一部を双方向古典チャネルを通して比較する．それらが正しく送受信されていれば，非常に高い確率で傍受者 Eve は存在しないことが確証でき，彼らが共有する暗号鍵をもちいて one-time pad が利用できる．

例 4.1 Alice と Bob のデータが以下のようであるとする：

Alice の送信コード	0	1	0	0	1	1	0	1	0	0	1	0
Alice の偏光	(1)	(2)	(1)	(2)	(2)	(1)	(2)	(1)	(2)	(2)	(1)	(1)
Bob の偏光	(1)	(2)	(2)	(1)	(2)	(2)	(1)	(2)	(1)	(2)	(2)	(1)
Bob の受信コード	0	1	?	?	1	?	?	?	?	0	?	0

(68)

ここに?は0か1のどちらかを表す．したがって列$0,1,1,0,0$を鍵として用いればよい．この鍵を知っているのはこの世でこの2人だけである．

一方，Eveが傍受しているとしよう．すると，かれらの測定結果は，たとえば

Aliceの送信コード	0	1	0	0	1	1	0	1	0	0	1	0
Aliceの偏光	(1)	(2)	(1)	(2)	(2)	(1)	(2)	(1)	(2)	(2)	(1)	(1)
Eveの偏光	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)	(1)	(2)
Eveの受信コード	0	1	0	0	?	?	?	?	?	0	1	?
Bobの偏光	(1)	(2)	(2)	(1)	(2)	(2)	(1)	(2)	(1)	(2)	(2)	(1)
Bobの受信コード	0	1	?	?	?	?	?	?	?	0	?	?

(69)

となる．5番目と12番目は2人が同じ偏光を用いたにも拘わらず，確率1/4で異なる結果となり，大量に量子ビットを送るとBobらはEveの存在を知ることができる．

4.3 量子ゲート

量子系の時間発展はSchrödinger方程式で記述される．系のノルムが保存するので，時間発展はユニタリーである．Uを時間発展の演算子とする．以下では，特にSchrödinger方程式を意識せず，必要な行列Uは常に存在するものとして話を進める．物理系におけるUの実現は重要な研究テーマであり，最後の節でその一部を紹介する．時間発展がユニタリーであることより，すべての量子ゲートは可逆となる．

4.3.1 簡単な量子ゲート

概念になれるために簡単な量子ゲートをいくつか紹介する．線型性から量子ゲートの任意の状態に関する作用は，その$|0\rangle, |1\rangle$に関する作用が指定されれば完全に定まる．ゲートI, X, Y, Zを定義しよう：

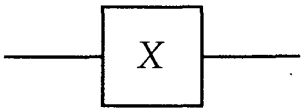
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} : |0\rangle \to |0\rangle, \quad |1\rangle \to |1\rangle \tag{70}$$

$$X \equiv \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} : |0\rangle \to |1\rangle, \quad |1\rangle \to |0\rangle \tag{71}$$

$$Y \equiv i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : |0\rangle \to -|1\rangle, \quad |1\rangle \to |0\rangle \tag{72}$$

$$Z \equiv \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} : |0\rangle \to |0\rangle, \quad |1\rangle \to -|1\rangle \tag{73}$$

Iは恒等変換，Xは否定(NOT)，Zは位相シフト，$Y = ZX$はXとZの組み合わせである．これらがユニタリーであることを確かめよ．1量子ビットゲートを箱で表し，その中に名前を入れる．たとえばXゲートを



と表す．ゲートの入力は左側，ゲートが作用した出力は右側から現れるものとする．

制御NOT(CNOT(controlled-NOT))ゲートは2量子ビットゲートで，量子計算で中心的な役割を果たす．これは第1量子ビット（制御ビット）が1のときは第2量子ビット（ターゲットビット）を反転し，第1量子ビットが0のときはそのまま通過させる．$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ を2量子ビットの基底とする．以下，これらを

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

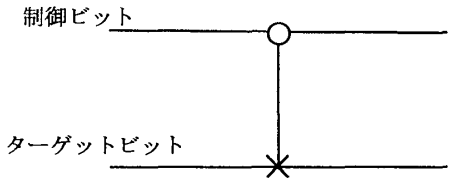
と表す．するとCNOTゲートは

$$\text{CNOT}: \begin{array}{l} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{array} \Leftrightarrow U_{\text{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{74}$$

と表される．CNOTはユニタリーで $U_{\text{CNOT}}^2 = I$ であることを確かめよ．

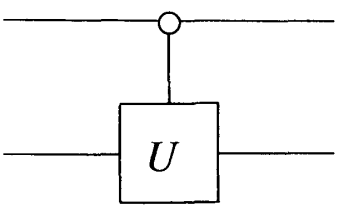
問 4.4 CNOTゲートは2つの1量子ビットゲートのテンソル積ではかけないことを示せ．

量子ゲートを図で表すと便利である．CNOTゲートを



と表す．ここに○は制御ビットを，×は条件付否定を表す．後で紹介するCCNOTゲートのように，制御ビットは複数あってもかまわない．また，制御ビットが0のときのみ，ターゲットビットを否定する制御ゲートも考えられる．このときは制御ビットに●を使い，通常の制御○と区別する．

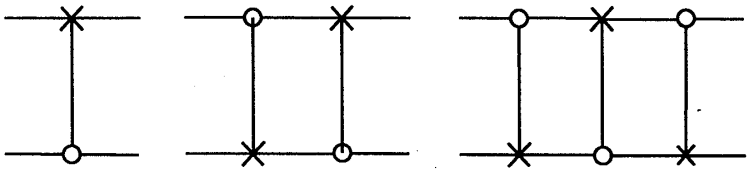
より一般に制御 U ゲートは制御ビットが $|1\rangle$ のときのみターゲットビットにユニタリー行列 U が作用する．これを図で



と表す．$U = X$ ととればCNOTゲートが得られる．

問 4.5 基底を $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ とする．

(1) “さかさま” CONT ゲート (a) の行列表現をもとめよ．

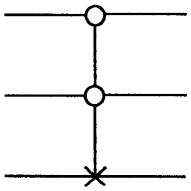


(a) (b) (c)

(2) 量子回路 (b) の行列表現を書き下し，その働きを解析せよ．

(3) 量子回路 (c) の行列表現を書き下し，その働きを解析せよ．

CCNOT (Controlled-Controlled-NOT) ゲートは3量子ビットに作用し，最初の2量子ビットがともに1のときのみ第3量子ビットが反転する．このゲートを



と図示する．

Walsh-Hadamard 変換

Hadamard 変換は

$$H: \quad |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{75}$$

で定義され，$|0\rangle$ や $|1\rangle$ から重ね合わせ状態を作る重要な変換である．H を行列で表すと

$$H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{76}$$

Hadamard ゲートを

と図示する．

Hadamard ゲートは多くの応用をもつ．H が $|0\rangle$ に作用すると，重ね合わせ状態 $(|0\rangle + |1\rangle)/\sqrt{2}$ が得られる．さらに n 量子ビット系の各量子ビットに H が作用すると 2^n 個のすべての状態の重

ね合わせが得られる：

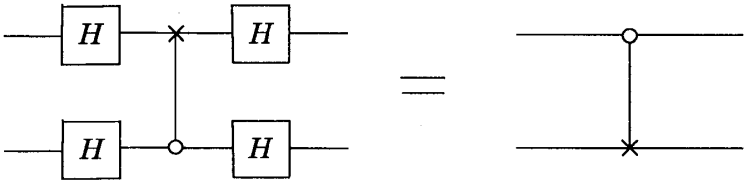
$$\begin{aligned}(H\otimes H\otimes\ldots\otimes H)|00\ldots0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\ldots\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\\ &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle \end{aligned} \tag{77}$$

このn量子ビットに作用する変換W_nは**Walsh変換**，または**Walsh-Hadamard変換**とよばれる：

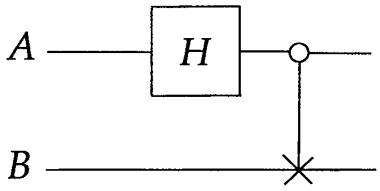
$$W_n=\underbrace{H\otimes H\otimes\ldots\otimes H}_{n\text{個}}. \tag{78}$$

問 4.6 W_nはユニタリーであることを示せ．

問 4.7 下図の左の量子ゲートは制御ビットとターゲットビットを交換するので右の量子ゲートに等しいことを示せ．



問 4.8 下図の量子回路を考えよう．



(79)

ただしAは第1番量子ビット，Bは第2番量子ビットである．入力$|00\rangle,|01\rangle,|10\rangle,|11\rangle$にたいする出力を求めよ．

4.4 No Cloning 定理

日常我々はフロッピーディスクやCD ROMなどにデータをコピーするが，未知の量子ビットはユニタリー操作ではコピー不可能である！

定理 4.1 (Wootters-Zurek) 未知の量子状態をユニタリー変換では複製できない．

証明 ある量子系のクローンを生成するユニタリー変換Uがあったとしよう．すなわちUは任意の状態$|a\rangle$に作用して$U:|a0\rangle\to|aa\rangle$を与える．ここに$|a0\rangle=|a\rangle\otimes|0\rangle$．定義から$U|a0\rangle=|aa\rangle$, $U|b0\rangle=|bb\rangle$．一方，Uの$|c\rangle=\frac{1}{\sqrt{2}}(|a\rangle+|b\rangle)$にたいする作用は

$$U|c0\rangle=\frac{1}{\sqrt{2}}(U|a0\rangle+U|b0\rangle)=\frac{1}{\sqrt{2}}(|aa\rangle+|bb\rangle)$$

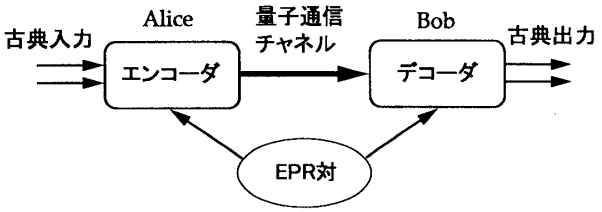


図 3: dense coding を用いた Alice から Bob への通信.

である．もし U が本当にクローンを生成するならば，$U|c0\rangle = |cc\rangle = \frac{1}{2}(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle)$ も満たさなければならないが，$|a\rangle$ と $|b\rangle$ を互いに線型独立な状態とするとこれは矛盾である．したがって，未知の状態をクローンするユニタリー変換は存在しない． ∎

問 4.9 U はクローンを実行するユニタリー演算子であるとする．すなわち任意の $|\psi\rangle, |\phi\rangle$ にたいし

$$|\Psi\rangle \equiv U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle, \quad |\Phi\rangle \equiv U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$$

となるものとする．
(1) $\langle\Psi|\Phi\rangle$ をすべての可能な方法で書き下せ．
(2) (1) の結果からこのような U は存在しないことを示せ．

4.5 Dense Coding と量子テレポーテーション

少数量子ビットの簡単な応用として**dense coding** と**量子テレポーテーション**を紹介する．dense coding は 1 対の EPR 対を利用し，Alice から Bob へ 2 ビットの古典情報を送る．EPR 対は前もって配布され，2 ビットの古典情報は 1 個の量子ビットが運ぶ．一方，量子テレポーテーションでは 2 古典ビットを用いて 1 個の量子ビットを転送する．一見すると量子テレポーテーションは no cloning 定理と矛盾するようであるが，もともとの状態は破壊されるので，クローンではない．いずれの場合ももつれた状態がキーワードである．Alice は Bob にある情報を送りたい．おのおのは前もって EPR 対 $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ の片方を配布されている．Alice はその第 1 量子ビットを Bob は第 2 量子ビットを持っているとしよう．

4.5.1 Dense coding

Alice: Alice は Bob に数 x, $0 \le x \le 3$ のひとつを送りたい（図 3）．x は $\{00, 01, 10, 11\}$ と 2 進法で表されている．Alice は x の値により $\{I, X, Y, Z\}$ のどれかを用いて彼女が持っている EPR 対の片割れに作用させる．彼女の量子ビットのみに作用させるということは，Bob がもっている量

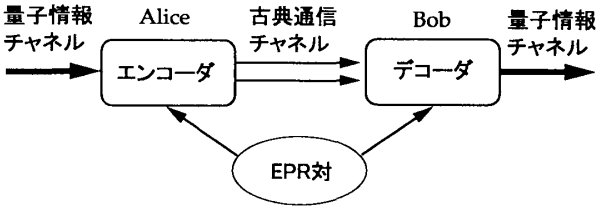


図 4: Alice は量子テレポーテーションで Bob に量子ビットを送信する．

子ビットには恒等変換 I を作用させることに他ならない．その結果は

$$\begin{array}{lll} x & \text{変換} & \text{変換後の状態} \\ 0=00 & |\psi_0\rangle=(I\otimes I)|\psi_0\rangle & \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \\ 1=01 & |\psi_1\rangle=(X\otimes I)|\psi_0\rangle & \frac{1}{\sqrt{2}}(|10\rangle+|01\rangle) \\ 2=10 & |\psi_2\rangle=(Y\otimes I)|\psi_0\rangle & \frac{1}{\sqrt{2}}(-|10\rangle+|01\rangle) \\ 3=11 & |\psi_3\rangle=(Z\otimes I)|\psi_0\rangle & \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle) \end{array} \tag{80}$$

となる．Alice は上の変換を実行した後，Bob に自分の量子ビットを送る．(上の右側の 4 状態は Bell 基底とよばれる.)

問 4.10 Bell 基底は 2 量子ビット系の正規直交系であることを示せ.

Bob: Bob は 2 量子ビットの第 1 ビットを制御ビット，第 2 ビットをターゲットビットとして CNOT ゲートを作用させる．その結果はテンソル積状態

$$\begin{array}{llll} \text{受け取った状態} & \text{CNOT の出力} & \text{第 1 量子ビット} & \text{第 2 量子ビット} \\ |\psi_0\rangle & \frac{1}{\sqrt{2}}(|00\rangle+|10\rangle) & \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) & |0\rangle \\ |\psi_1\rangle & \frac{1}{\sqrt{2}}(|11\rangle+|01\rangle) & \frac{1}{\sqrt{2}}(|1\rangle+|0\rangle) & |1\rangle \\ |\psi_2\rangle & \frac{1}{\sqrt{2}}(-|11\rangle+|01\rangle) & \frac{1}{\sqrt{2}}(-|1\rangle+|0\rangle) & |1\rangle \\ |\psi_3\rangle & \frac{1}{\sqrt{2}}(|00\rangle-|10\rangle) & \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) & |0\rangle \end{array} \tag{81}$$

となる．したがって Bob は第 2 量子ビットを独立に測定することができる．第 2 ビットが 0 (1) であれば x は 0 か 3 (1 か 2) である．最後に Bob が第 1 ビットに Hadamard 変換 H を施すと

$$\begin{array}{lll} \text{受け取った状態} & \text{第 1 量子ビット} & H \text{ を作用させた後の第 1 量子ビット} \\ |\psi_0\rangle & \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) & \frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)]=|0\rangle \\ |\psi_1\rangle & \frac{1}{\sqrt{2}}(|1\rangle+|0\rangle) & \frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)+\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)]=|0\rangle \\ |\psi_2\rangle & \frac{1}{\sqrt{2}}(-|1\rangle+|0\rangle) & \frac{1}{\sqrt{2}}[-\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)+\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)]=|1\rangle \\ |\psi_3\rangle & \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) & \frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)-\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)]=|1\rangle \end{array} \tag{82}$$

となる．したがって第 1 ビットを観測することにより，Bob は 2 古典ビット x を確実に知る.

4.5.2　量子テレポーテーション

量子テレポーテーションは「未知の量子状態を古典ビットを用いて送信し，受信した人が元の量子状態を再現する」プロセスである (図 4)．元の状態は破壊されてしまうので，これは no cloning

定理には反しない．量子テレポーテーションは実験室ではすでに実現している．

Alice: Alice は未知の量子状態 $|\phi\rangle = a|0\rangle + b|1\rangle$ をもっており，その状態を古典チャネルを通して Bob に送りたい．両者は事前に EPR 状態

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{4.20}$$

の一方をそれぞれ配布されている．彼らの初期状態は

$$\begin{aligned} |\phi\rangle \otimes |\psi_0\rangle &= \frac{1}{\sqrt{2}}[a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)] \\ &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle), \end{aligned} \tag{83}$$

である．最初の 2 ビットは Alice に属し，最後の 1 ビットは Bob に属する．Alice は彼女の 2 つの量子ビットに CNOT を作用させた後 $H \otimes I$ を作用させる（Bob の量子ビットには I を作用させる）：

$$\begin{aligned} &(H \otimes I \otimes I)(\mathrm{CNOT} \otimes I)(|\phi\rangle \otimes |\psi_0\rangle) \\ &= \frac{1}{2}[a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)] \\ &= \frac{1}{2}[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)]. \end{aligned} \tag{84}$$

Alice が彼女の 2 量子ビットを測定すると，彼女は $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ のどれかを等確率 1/4 で観測する．Alice の観測結果に応じて Bob の量子ビットは $a|0\rangle + b|1\rangle, a|1\rangle + b|0\rangle, a|0\rangle - b|1\rangle$ または $a|1\rangle - b|0\rangle$ に収縮する．Alice は Bob に彼女の測定結果を古典チャネルを通して伝える．Alice は測定により彼女がもっていた状態 $|\phi\rangle$ を完全に破壊したことに注意しよう．したがってこれはクローンではない．

Bob: 2 個の古典ビットを受信した Bob は，彼のもっている量子ビットの状態を知ることができる：

受信したデータ	Bob の状態	デコードするゲート
00	$a\|0\rangle + b\|1\rangle$	I
01	$a\|1\rangle + b\|0\rangle$	X
10	$a\|0\rangle - b\|1\rangle$	Z
11	$a\|1\rangle - b\|0\rangle$	Y

(85)

Bob は彼の量子ビットに上に示したデコードゲートを施すことにより最初 Alice がもっていた状態 $|\phi\rangle$ を再現することができる．例えば Alice が 10 を送ったとしよう．すると Bob は彼の量子ビットに Z を施して $|\phi\rangle$ を再現する：

$$Z:\ (a|0\rangle - b|1\rangle) \to (a|0\rangle + b|1\rangle) = |\phi\rangle.$$

Alice が送ったデータが 00, 01, 11 の時にも Bob は正しく $|\phi\rangle$ を再現することを各自確かめよ．

5　量子コンピュータ

本章ではいくつかの例を挙げながら量子コンピュータの概念を説明する．同時に量子コンピュータのパワーも明らかにする．

まず，量子コンピュータにたいする2つのアプローチについてコメントする．一つは量子 Turing 機械 (QTM) に基づくもので，他方はすでに現れた量子ゲートや量子回路に基づくものである．これらは同値であることが証明されるので，以下では量子論理ゲートに基づく解析を行う．

5.1　量子コンピュータ

定義 5.1 $\mathcal{H} = \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ を n 量子ビットのヒルベルト空間とする．これを**レジスター**ともよぶ．U を $\mathcal{H}$ に作用するユニタリー演算子，$\{M_m\}$ を測定演算子の集合とする．集合 $\{\mathcal{H}, U, \{M_m\}\}$ を**量子コンピュータ**とよぶ．U は量子アルゴリズムとも言われる．

“量子ゲート”, “量子回路”, “量子コンピュータ” の区別はあまりクリアではないが，一般に量子コンピュータに比べ量子ゲートは簡単である場合が多い．

古典コンピュータと量子コンピュータの大きな違いを3つ指摘する．

(1) 古典コンピュータが自然に朽ち果てるにはかなりの時間が必要であるが，量子コンピュータは環境と相互作用してその量子状態が崩壊してしまう．これを**デコヒーレンス**という．デコヒーレンスが生じる時間は物理系によって異なるが，問題はその絶対的な時間ではなく，それをゲートの動作時間で割った量，すなわちデコヒーレンスが顕著となる前に何ステップの計算ができるかである．

(2) 古典コンピュータでは情報（ビット）は情報処理中に入力デバイスから出力デバイスまで論理ゲートの中を動き回る．一方，量子コンピュータでは情報はレジスターの中にとどまり，論理ゲート（ユニタリー行列）が次々にレジスターに作用する．

(3) これらの論理ゲートは，式 (43) において，ハミルトニアンがもっている外部パラメタ，例えば外部磁場の振動数や振幅，それが印加されている時間などを調節して実現される．これらのパラメタはいずれもアナログ量であり，その意味で量子コンピュータはアナログ的要素をもっている．

5.2　古典論理ゲートとの対応

量子論理ゲートは古典論理ゲートを完全に再現する．ここで，量子ゲートに慣れるために古典論理ゲートがいかにユニタリーゲートとして現されるかを調べよう．

5.2.1 NOT ゲート

古典論理関数

$$\mathrm{NOT}(x) = \neg x = \begin{cases} 0 & (x=1) \\ 1 & (x=0) \end{cases} \tag{86}$$

を考えよう．ここに $\neg x$ は x の否定．量子計算では状態は $\mathbb{C}^2$ に属し，x の否定を実現するユニタリー行列は $X = \sigma_x$ である：

$$X|x\rangle = |\neg x\rangle = |\mathrm{NOT}(x)\rangle, \ (x = 0, 1). \tag{87}$$

実際 $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$ となる．$|x\rangle$ は入力，$|\mathrm{NOT}(x)\rangle$ は（測定される前の）出力である．さて，測定を実行しよう．測定演算子 $P_1 = |1\rangle\langle 1|$ を考えよう．P_1 は固有値 $0, 1$ と対応する固有ベクトル $|0\rangle$ と $|1\rangle$ をもつ．入力が $|0\rangle$ ならば出力は $|1\rangle$ で，測定は確率 1 で 1 を与える．一方入力が $|1\rangle$ ならば出力は $|0\rangle$ で，測定は確率 0 で 1 を与える（言い換えると確率 1 で 0 を与える.）

問 5.1 任意の 2×2 ユニタリー行列は

$$U = e^{i\theta/2} \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}, \quad (|a|^2 + |b|^2 = 1) \tag{88}$$

とかけることを示せ．これを用いて X は $U|0\rangle = |1\rangle$ および $U|1\rangle = |0\rangle$ を満たす唯一のユニタリー行列であることを示せ．

5.2.2 XOR

量子ゲートは可逆でなければならないので，古典的な XOR : $x, y \mapsto x \oplus y$ $(x, y \in \{0, 1\})$ のようなユニタリーゲートは存在しない．ここに

$$\mathrm{XOR}(x, y) \equiv x \oplus y = \begin{cases} 1 & x + y = 1 \\ 0 & \text{それ以外} \end{cases}$$

即ち $\mathrm{XOR}(x, y) = x + y \pmod 2$ である．あきらかにこれは逆をもたないが x を残すことによって可逆にできる：

$$f(x, y) = (x, x \oplus y), \quad x, y \in \{0, 1\}. \tag{89}$$

この f も XOR という．この作用を実行する量子ゲートは CNOT ゲート $U_{\mathrm{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$ に他ならない．

問 5.2 CNOT ゲートに対し

$$U_{\mathrm{CNOT}}(|x\rangle \otimes |y\rangle) \equiv U_{\mathrm{CNOT}}|x, y\rangle = |x, x \oplus y\rangle \tag{90}$$

を示せ．

問 5.3 以下の作用を実行するユニタリーゲート V を書き下せ：

$$V|x,y\rangle = |x \oplus y, y\rangle, \quad x,y \in \{0,1\}. \tag{91}$$

XOR は CCNOT からも構成できる．実際第 1 ビットが $|1\rangle$ に固定されていると

$$\mathrm{CCNOT}|1,x,y\rangle = |1,x,x \oplus y\rangle. \tag{92}$$

5.2.3 AND

古典的な AND は

$$\mathrm{AND}(x,y) \equiv x \wedge y \equiv \begin{cases} 1 & x=y=1 \\ 0 & \text{その他} \end{cases} \qquad x,y \in \{0,1\} \tag{93}$$

で定義される．これも可逆ではないので XOR と同様の対策をとらなければならない．

論理関数

$$f(x,y,0) \equiv (x,y,x \wedge y) \tag{94}$$

を定義しよう．可逆であるためには x だけでなく x と y の両方を残さなければならない：$x = x \wedge y = 0$ には $x = y = 0$ と $x = 0,\ y = 1$ の可能性がある．f を実現するユニタリーゲートを具体的に構成すると

$$\begin{aligned} U_{\mathrm{AND}} &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes I + |0\rangle\langle 0| \otimes |1\rangle\langle 1| \otimes I \\ &\quad + |1\rangle\langle 1| \otimes |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes |1\rangle\langle 1| \otimes X. \end{aligned} \tag{95}$$

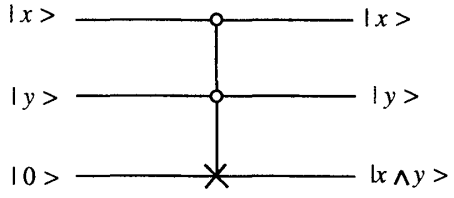
実際

$$\begin{aligned} U_{\mathrm{AND}}|x,y,0\rangle &= (|0\rangle\langle 0|x\rangle) \otimes (|0\rangle\langle 0|y\rangle) \otimes |0\rangle + (|0\rangle\langle 0|x\rangle) \otimes (|1\rangle\langle 1|y\rangle) \otimes |0\rangle \\ &\quad + (|1\rangle\langle 1|x\rangle) \otimes (|0\rangle\langle 0|y\rangle \otimes |0\rangle + (|1\rangle\langle 1|x\rangle) \otimes (|1\rangle\langle 1|y\rangle) \otimes (X|0\rangle) \\ &= \delta_{x0}\delta_{y0}|x,y,0\rangle + \delta_{x0}\delta_{y1}|x,y,0\rangle + \delta_{x1}\delta_{y0}|x,y,0\rangle + \delta_{x1}\delta_{y1}|x,y,1\rangle \\ &= (\delta_{x0}\delta_{y0} + \delta_{x0}\delta_{y1} + \delta_{x1}\delta_{y0})|x,y,0\rangle + \delta_{x1}\delta_{y1}|x,y,1\rangle. \end{aligned}$$

したがって第 3 ビットは $x = y = 1$ のときのみ 1 でそれ以外は 0 となる．即ち

$$U_{\mathrm{AND}}|x,y,0\rangle = |x,y,x \wedge y\rangle, \quad x,y \in \{0,1\}. \tag{96}$$

以上の議論から AND ゲートは図式的に



とかかれる．やはり CCNOT が AND を実現するのである．

5.2.4 OR

古典的なORは

$$\mathrm{OR}(x,y) = x \vee y = \begin{cases} 0 & x = y = 0 \\ 1 & \text{その他} \end{cases} \qquad x, y \in \{0,1\}. \tag{97}$$

で定義され，やはり非可逆である．そこで

$$f(x,y,0) \equiv (\neg x, \neg y, x \vee y), \quad x, y \in \{0,1\} \tag{98}$$

を定義し，これをやはりORとよぶ．(最初の2ビットは否定されているが，これは本質的ではない．後に示す基本ゲートからの構成上そうなっているだけである．)

f を表すユニタリーゲートは

$$U_{\mathrm{OR}} = |00\rangle\langle 11| \otimes X + |01\rangle\langle 10| \otimes X + |10\rangle\langle 01| \otimes X + |11\rangle\langle 00| \otimes I \tag{99}$$

である．ここに $|01\rangle = |0\rangle \otimes |1\rangle, \langle 10| = \langle 1| \otimes \langle 0|$ etc.

問 5.4 上の行列 U_{OR} は

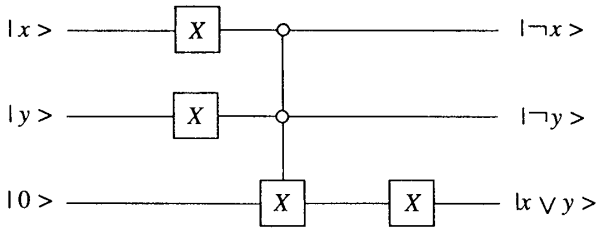
$$U_{\mathrm{OR}}|x,y,0\rangle = |\neg x, \neg y, x \vee y\rangle, \quad x, y \in \{0,1\} \tag{100}$$

を満たすことを示せ．

さて，ORゲートになぜ否定が現れるか説明しよう．ORはNOTとANDを使って

$$x \vee y = \neg(\neg x \wedge \neg y) \tag{101}$$

と表される (de Morganの定理)．すでにNOTとANDは構成されているので，これをORの構成に利用する．上の等式から



が推察される．この図から得られるユニタリー行列は

$$\begin{aligned} U \;=\; & (I \otimes I \otimes X) \cdot (|00\rangle\langle 00| \otimes I + |01\rangle\langle 01| \otimes I + |10\rangle\langle 10| \otimes I + |11\rangle\langle 11| \otimes X) \\ & \cdot (X \otimes X \otimes I). \end{aligned} \tag{102}$$

但し最初のファクターは第3層，2番目のファクター (CCNOT) は第2層 (AND) で3番目のファクターは第1層である．行列の積をとるとこれが (99) に帰着することは各自確かめよ．

ORはXとCCNOTゲートより構成され，X自身も第1，第2入力ビットを$|1\rangle$にとることによりCCNOTゲートから構成されることに注意せよ．

[注: ゲート$V_{\rm OR}|x,y,0\rangle = |x,y,x\vee y\rangle$が必要であれば$U_{\rm OR}$の後に$X\otimes X\otimes I$を実行すればよい：$V_{\rm OR} = (X\otimes X\otimes I)U_{\rm OR}$．]

問 5.5 NANDゲートはCCNOTゲートから構成されることを示せ．ただし古典的に

$$\mathrm{NAND}(x,y) = \begin{cases} 0 & x=y=1 \\ 1 & \text{その他} \end{cases} \qquad x,y\in\{0,1\}. \tag{103}$$

まとめると，すべての古典論理ゲートNOT, AND, OR, XOR, NANDはCCNOTから構成されることが分かった．したがって，すべての古典計算は量子計算の特別な場合として実現される．しかし量子計算が扱う情報の単位は量子ビットであり，古典的な0,1状態はそのごく限られた部分集合であることに注意されたい..

5.2.5 SWAP

SWAPはxとyを交換する：

$$\mathrm{SWAP}(x,y)\equiv(y,x),\quad x,y\in\{0,1\}. \tag{104}$$

$|x,y\rangle$に作用し，それを交換するユニタリー行列Sは$S|x,y\rangle = |y,x\rangle$, $x,y\in\{0,1\}$を満たす．これは具体的に

$$S = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| \tag{105}$$

と表される．

問 5.6 上のSは

$$S = (|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X)\cdot(I\otimes|0\rangle\langle 0| + X\otimes|1\rangle\langle 1|)\cdot(|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X)$$

と書かれることを示せ．これから問4.5 (3)のゲートがSWAPゲートであることが分かる．

5.3 量子回路

前節で紹介された簡単なゲートを組み合わせると，さらに複雑な働きをする回路が作られる．そのような量子回路の例をいくつか紹介しよう．

U_1, U_2を任意のユニタリー行列とする．すると条件付ユニタリー変換

$$U = |0\rangle\langle 0|\otimes U_1 + |1\rangle\langle 1|\otimes U_2 \tag{106}$$

は再びユニタリーである．実際

$$\begin{aligned} UU^\dagger &= (|0\rangle\langle 0|\otimes U_1 + |1\rangle\langle 1|\otimes U_2)(|0\rangle\langle 0|\otimes U_1^{-1} + |1\rangle\langle 1|\otimes U_2^{-1}) \\ &= |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes I = I\otimes I. \end{aligned}$$

CNOT ゲート $U_{\mathrm{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$ はそのような変換の例である．このような変換は 2×2 行列のテンソル積ではかけない．

CCNOT ゲート (Toffoli ゲートともいう) も条件付変換の例である：

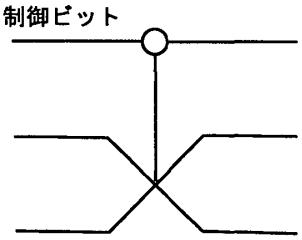
$$U_{\mathrm{CCNOT}} = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes \mathrm{CNOT} \tag{107}$$

これは上に見たように古典論理ゲートをすべて再現する．

Fredkin ゲート F は，制御ビットが 1 のときのみ第 2，第 3 ビットを交換する制御 SWAP ゲート

$$F = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes S \tag{108}$$

である．ただし S は SWAP ゲート.. F も古典論理ゲートをすべて再現する．Fredkin ゲートは



と図示されることもある．

問 5.7 NOT, AND, OR はそれぞれ 1 個の Fredkin ゲートから構成されることを示せ．(NAND と XOR は 2 個以上の Fredkin ゲートを必要とする．)

5.4 万能量子ゲート

いかなる古典論理ゲートも例えば AND, NOT, XOR から構成される．このようなゲートは古典計算の万能 (universal) ゲートとよばれる．上に見たように CCNOT ゲートをもちいるとすべての古典論理回路を再現することができる．ではすべての量子回路，すなわちすべてのユニタリー行列を構成することができる**万能量子ゲート**の組は何だろうか． 以下で

(1) すべての 1 量子ビットゲート，すなわちユニタリー群 U(2) 全体と
(2) CNOT ゲート

が量子回路にたいする万能量子ゲートであることを示す．主定理の前に以下の補題を証明する．

補題 5.1 U は $\mathbb{C}^d$ に作用するユニタリー行列とすると，$N = d(d-1)/2$ 個の**レベル 2** のユニタリー行列 $U_1, U_2, \ldots, U_N$ が存在し

$$U = U_1 U_2 \ldots U_N \tag{109}$$

と分解できる．[注: レベル 2 のユニタリー行列とは高々2 つの成分の間でのみその作用が自明ではないユニタリー行列をさす．V をレベル 2 のユニタリー行列とする．するとある行列要素

$V_{aa}, V_{ab}, V_{ba}, V_{bb}$ は自明でないが，それ以外の行列要素は単位行列と等しい．このような行列の例は

$$V = \begin{pmatrix} \alpha^* & 0 & 0 & \beta^* \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\beta & 0 & 0 & \alpha \end{pmatrix}, \quad (|\alpha|^2 + |\beta|^2 = 1).$$

ただし $a = 1, b = 4$ ととった．自明でない行列要素 V_{ij} から構成される行列は U(2) の元である．]

証明: まず $d = 3$ の場合を調べよう．

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}$$

をユニタリー行列とする．レベル 2 のユニタリー行列 U_1, U_2, U_3 で

$$U_3 U_2 U_1 U = I$$

を満たすものを探す．これから $U = U_1^\dagger U_2^\dagger U_3^\dagger$ と求められる．($U_k^\dagger$ もレベル 2 のユニタリー行列である.) このような U_k を具体的に構成しよう．

(i) まず

$$U_1 = \begin{pmatrix} \frac{a^*}{u} & \frac{b^*}{u} & 0 \\ -\frac{b}{u} & \frac{a}{u} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad u = \sqrt{|a|^2 + |b|^2}$$

とする．(U_1 がユニタリーであることを確かめよ.) これから

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix}$$

となる．a' から j' は複素数である．第 2 行の第 1 要素は 0 となったことに注意．

(ii) 次に

$$U_2 = \begin{pmatrix} \frac{a'^*}{u'} & 0 & \frac{c'^*}{u'} \\ 0 & 1 & 0 \\ -\frac{c'}{u'} & 0 & \frac{a'}{u'} \end{pmatrix} = \begin{pmatrix} a'^* & 0 & c'^* \\ 0 & 1 & 0 \\ -c' & 0 & a' \end{pmatrix}, \quad u' = \sqrt{|a'|^2 + |c'|^2} = 1$$

とする．$u' = 1$ は $U_1 U$ のユニタリー性から得られる．すると

$$U_2 U_1 U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix}$$

となる．等式 $d'' = g'' = 0$ は $U_2 U_1 U$ がユニタリーで第 1 行が 1 に規格化されていることから導かれる．

(iii) 最後に

$$U_3 = (U_2U_1U)^\dagger = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix}$$

とすると定義により明らかに $U_3U_2U_1U = I$. したがって $d = 3$ にたいし補題が示された.

U は任意の $\mathbb{C}^d$ に作用するユニタリー行列とする. 先ほどの議論を繰り返すことによりレベル2のユニタリー行列 $U_1, U_2, \ldots, U_{d-1}$ で

$$U_{d-1}\ldots U_2U_1U = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & * & * & \ldots & * \\ 0 & * & * & \ldots & * \\ & & \ldots & \ldots & \\ 0 & * & * & \ldots & * \end{pmatrix}$$

を満たすものが存在する. これを実現する行列 $\{U_k\}$ の個数は第1列の0の個数, すなわち $(d-1)$ に等しい.

このプロセスを残った $(d-1)\times(d-1)$ ブロック行列に適用すると $(d-2)$ 個のレベル2のユニタリー行列をうまく選べば $(d-2)\times(d-2)$ のブロックが残る. これを繰り返すと U はレベル2のユニタリー行列の積で $U = V_1V_2\ldots V_k$ と表される. ここに $k \leq (d-1)+(d-2)+\ldots+1 = d(d-1)/2$.

∎

問 5.8 U を任意の 4×4 ユニタリー行列とする.

$$U_3U_2U_1U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix}$$

となるようなレベル2のユニタリー行列 U_1, U_2, U_3 を求めよ.

問 5.9

$$U = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \tag{110}$$

とする. U をレベル2のユニタリー行列の積でかけ.

n 量子ビット系に作用するユニタリー行列を考える. この行列は高々 $2^n(2^n-1)/2 = 2^{n-1}(2^n-1)$ 個のレベル2のユニタリー行列の積に分解される.

定理 5.1 (Barenco *et al.* [8]) すべての量子ビット・ゲートと CNOT ゲートは universal である. すなわち n 量子ビット系に作用する任意のユニタリーゲートは1量子ビットゲートと CNOT ゲートで構成される.

証明: 補題のおかげで，この定理をレベル2のユニタリー行列について証明すれば十分である．U を n 量子ビットの中で $|s\rangle$ と $|t\rangle$ だけに作用するレベル2のユニタリー行列とする．ここで $s = s_{n-1}2^{n-1} + \ldots + s_1 2 + s_0$ と $t = t_{n-1}2^{n-1} + \ldots + t_1 2 + t_0$ を s, t の2進数表示とする．$\tilde{U}$ を U の非自明な要素から構成される 2×2 ユニタリー行列とすると $\tilde{U}$ は $\{|s\rangle, |t\rangle\}$ の1量子ビットに作用するユニタリー行列と見ることができる．

STEP 1: $(U \to \tilde{U})$

一般に無関係な基底ベクトル $|s\rangle, |t\rangle$ は次の "**Gray コード**" で1量子ビットを表しているとみなす事ができる．2つの2進数コード $s = s_{n-1} \ldots s_1 s_0$ と $t = t_{n-1} \ldots t_1 t_0$ にたいし s, t を結ぶ Gray コードとは2進数の列 $\{g_1, \ldots, g_m\}$ で隣り合う g_k と g_{k+1} は正確に1ビットだけ異なる．また境界条件 $g_1 = s$ と $g_m = t$ を満たしている．例えば $s = 10010$ and $t = 11011$ としよう．s と t を結ぶ Gray コードの例は

$$\begin{aligned} s = g_1 &= 10010 \\ g_2 &= 11010 \\ g_3 &= 11011 = t. \end{aligned}$$

この構成から s と t が p ビットだけ異なれば，最も短い Gray コードは $p+1$ の元からなっていることは明らかであろう．また s と t が n 桁であれば s と t は高々 n ビット異なるので $m \leq (n+1)$ となる．

これらの準備を元に U を構成しよう．基本的方針は次の変換

$$|s = g_1\rangle \to |g_2\rangle \to \ldots \to |g_{m-1}\rangle \tag{111}$$

を実現するゲートの列を見つけることである．すると g_{m-1} と g_m は1ビットしか違わないのでこれらを $\tilde{U}$ が作用する1量子ビットとみなす事ができる．$\tilde{U}$ が作用した後最初のゲートの列を反転させることにより $|g_{m-1}\rangle \to |g_{m-2}\rangle \to \ldots \to |g_1\rangle$ とすることができる．各ステップは以前紹介した単純なゲートを使って構成できる．

例として3量子ビット系を考える．基底は binary 基底 $\{|000\rangle, |001\rangle, \ldots, |111\rangle\}$ である．

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}, \quad (a, b, c, d \in \mathbb{C}) \tag{112}$$

をレベル2のユニタリー行列とする．U は $|000\rangle$ と $|111\rangle$ が張る部分空間においてのみ自明ではない．U のユニタリー性から行列

$$\tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \tag{113}$$

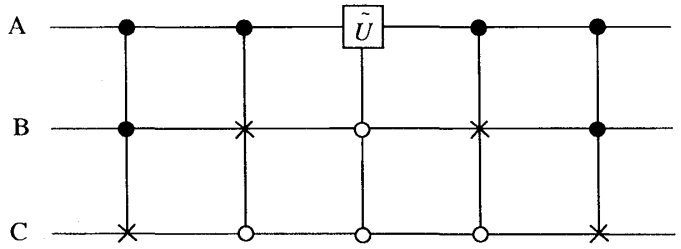


図 5: ゲート U を実現する量子回路の例.

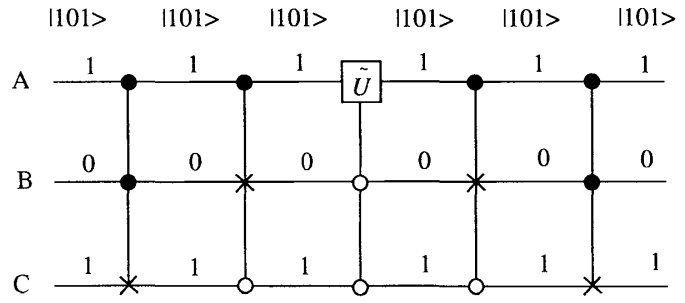


図 6: ゲート U はベクトル $|101\rangle$ には何ら作用しない.

もユニタリーとなる. 000 と 111 を結ぶ Gray コードの例は

$$\begin{array}{rccc} & A & B & C \\ g_1 = & 0 & 0 & 0 \\ g_2 = & 0 & 0 & 1 \\ g_3 = & 0 & 1 & 1 \\ g_4 = & 1 & 1 & 1 \end{array} \tag{114}$$

である. g_3 と g_4 は最初の量子ビット (A) しか違わないので, g_1 を g_3 までもってきて $\tilde{U}$ を量子ビット A に作用させればよい. ただし 2, 3 番目の量子ビットは $|11\rangle$ にあるものとする. すなわちターゲットビットが A で制御ビットが B と C の制御 $\tilde{U}$ ゲートに他ならない. この制御 $\tilde{U}$ ゲートが実行された後 $|g_3\rangle = |011\rangle$ を $|000\rangle$ まで $|011\rangle \to |001\rangle \to |000\rangle$ と戻さなければならない. これを図 5 のように表す. ここに • は否定制御ビット (制御ビットが 0 のときにみ制御が起こる) である. これが実際 U ゲートを実現していることを確かめよう. 入力が $|101\rangle$ であるとしよう. 図 6 はこのゲートが入力をそのまま出力することを示している. 一方, 入力 $\alpha|000\rangle + \beta|111\rangle$ にたいす

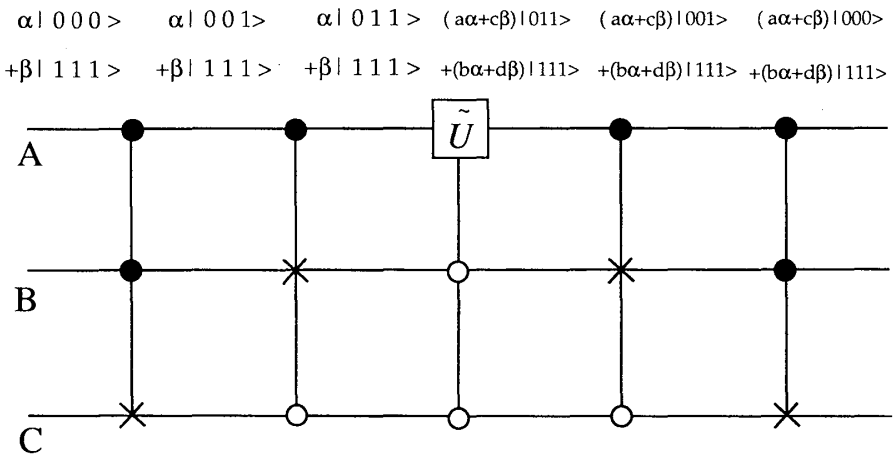


図 7: $U(\alpha|000\rangle + \beta|111\ \rangle) = [(\alpha a + \beta c)|000\rangle + (\alpha b + \beta d)|111\rangle]$ となる.

る U の作用は

$$U(\alpha|000\rangle + \beta|111\ \rangle) = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha a + \beta c \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \alpha b + \beta d \end{pmatrix}.$$

図 5 の回路を用いると，その結果は図 7 に示すように同じとなる.

この構成は任意のレベル 2 のユニタリー行列 U へ一般化できる．次に，上の量子回路は 1 量子ビットゲートと CNOT ゲートで実現されることを示す.

問 4.11 次のユニタリー行列を実現する量子回路を求めよ：

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{pmatrix}. \tag{115}$$

STEP 2

任意の $U \in \mathrm{U}(2)$ にたいし，制御 U ゲートは高々 4 個の 1 量子ビットゲートと 2 個の CNOT ゲートから構成できることを示す．まず補題いくつかを証明する.

補題 5.2 $U \in \mathrm{SU}(2)$ とし

$$R_z(\alpha) = \exp(i\alpha\sigma_z/2) = \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix},$$
$$R_y(\beta) = \exp(i\beta\sigma_y/2) = \begin{pmatrix} \cos(\beta/2) & \sin(\beta/2) \\ -\sin(\beta/2) & \cos(\beta/2) \end{pmatrix}$$

とすると $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$ となるような $\alpha, \beta, \gamma \in \mathbb{R}$ が存在する.

証明: 簡単な計算の後に

$$R_z(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} e^{i(\alpha+\gamma)/2}\cos(\beta/2) & e^{i(\alpha-\gamma)/2}\sin(\beta/2) \\ -e^{i(-\alpha+\gamma)/2}\sin(\beta/2) & e^{-i(\alpha+\gamma)/2}\cos(\beta/2) \end{pmatrix} \tag{116}$$

が得られる. $U \in \mathrm{SU}(2)$ であるから

$$U = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} = \begin{pmatrix} \cos\theta e^{i\lambda} & \sin\theta e^{i\mu} \\ -\sin\theta e^{-i\mu} & \cos\theta e^{-i\lambda} \end{pmatrix} \tag{117}$$

とかかれる. ただし $|a|^2 + |b|^2 = 1$ を用いた. したがって

$$\theta = \frac{\beta}{2}, \lambda = \frac{\alpha+\gamma}{2}, \mu = \frac{\alpha-\gamma}{2} \tag{118}$$

ととればよい. ∎

補題 5.3 $U \in \mathrm{SU}(2)$ とすると, $A, B, C \in \mathrm{SU}(2)$ が存在して $U = AXBXC$ かつ $ABC = I$ とできる. ただし $X = \sigma_x$.

証明: 補題 5.2 からある $\alpha, \beta, \gamma \in \mathbb{R}$ が存在して $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$. そこで

$$A = R_z(\alpha)R_y\left(\frac{\beta}{2}\right), B = R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right), C = R_z\left(-\frac{\alpha-\gamma}{2}\right)$$

とすると

$$\begin{aligned} AXBXC &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)XR_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)XR_z\left(-\frac{\alpha-\gamma}{2}\right) \\ &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)\left[XR_y\left(-\frac{\beta}{2}\right)X\right]\left[XR_z\left(-\frac{\alpha+\gamma}{2}\right)X\right]R_z\left(-\frac{\alpha-\gamma}{2}\right) \\ &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(\frac{\beta}{2}\right)R_z\left(\frac{\alpha+\gamma}{2}\right)XR_z\left(-\frac{\alpha-\gamma}{2}\right) \\ &= R_z(\alpha)R_y(\beta)R_z(\gamma) = U \end{aligned}$$

となる. ここで $X^2 = I$ および $X\sigma_{y,z}X = -\sigma_{y,z}$ を用いた.

また

$$ABC = R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)R_z\left(-\frac{\alpha-\gamma}{2}\right) = R_z(\alpha)R_y(0)R_z(-\alpha) = I$$

も確かめられる. ∎

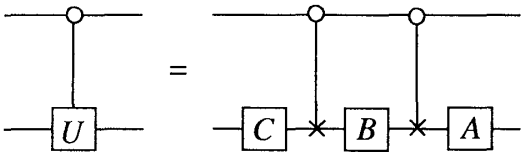


図 8: 制御 U ゲートは 1 量子ビットゲートと CNOT ゲートで実現できる.

補題 5.4 $U \in \mathrm{SU}(2)$ が $U = AXBXC$ と分解されたとすると制御 U ゲートは高々 3 個の 1 量子ビットゲートと 2 個の CNOT ゲートで実現される (図 8).

証明: これはほとんど自明である. 制御ビットが 0 のとき, ターゲットビット $|\psi\rangle$ には C, B, A が作用し $|\psi\rangle \mapsto ABC|\psi\rangle = |\psi\rangle$ となるが, 制御ビットが 1 のときは $|\psi\rangle \mapsto AXBXC|\psi\rangle = U|\psi\rangle$ となる.

より形式的には, $\mathrm{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$ から $(I \otimes A)\mathrm{CNOT}(I \otimes B)\mathrm{CNOT}(I \otimes C) = |0\rangle\langle 0| \otimes ABC + |1\rangle\langle 1| \otimes AXBXC = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$ が示され補題が証明される. ∎

これまでのところ $U \in \mathrm{SU}(2)$ としてきた. 一般の U ゲート ($U \in \mathrm{U}(2)$) を実現するには位相も考慮しなければならない.

補題 5.5

$$\Phi(\phi) = e^{i\phi} I = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

および

$$D = R_z(-\phi)\Phi\left(\frac{\phi}{2}\right) = \begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} \begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

とすると制御 $\Phi(\phi)$ ゲートは

$$\mathrm{C}\Phi(\phi) = D \otimes I \tag{119}$$

で与えられる.

証明: 左辺は

$$\begin{aligned} \mathrm{C}\Phi(\phi) &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \Phi(\phi) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\phi} I \\ &= |0\rangle\langle 0| \otimes I + e^{i\phi}|1\rangle\langle 1| \otimes I \end{aligned}$$

であるが, 右辺は

$$\begin{aligned} D \otimes I &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \otimes I = \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \right] \otimes I \\ &= \left[|0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1| \right] \otimes I = \mathrm{C}\Phi(\phi) \end{aligned}$$

となり補題が証明された. ∎

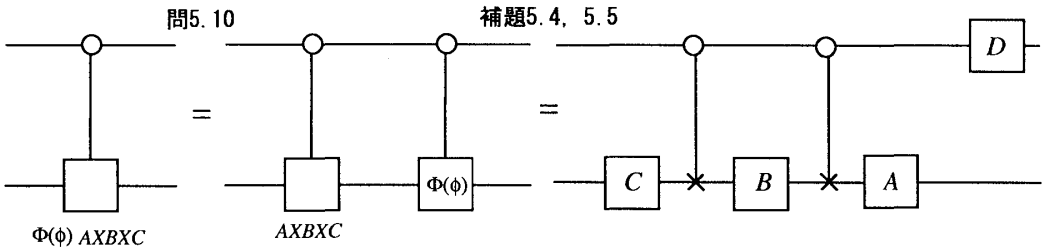
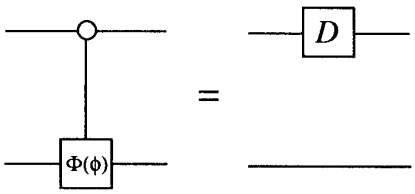
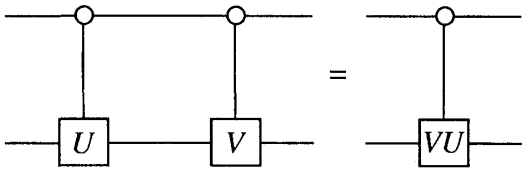


図 9: 制御 U ゲートは高々 4 個の 1 量子ビットゲートと 2 個の CNOT ゲートで実現できる.

この補題 $\mathrm{C}\Phi(\phi) = D \otimes I$ は以下のように図示される.



問 5.10 制御 U ゲートと制御 V ゲートを考える. 制御 U の後に制御 V ゲートが作用すると, その結果は制御 VU ゲートとなることを示せ.



CVCU = C(VU).

命題 5.1 $U \in \mathrm{U}(2)$ とすると, 制御 U ゲート (CU) は高々4 個の 4 量子ビットゲートと 2 個の CNOT ゲートで実現される (図 9).

証明: $U = \Phi(\phi)AXBXC$ とする. 上の問から制御 U ゲートは制御 $\Phi(\phi)$ ゲートと制御 $AXBXC$ ゲートの積で書かれる. さらに 補題 5.5 から制御 $\Phi(\phi)$ ゲートは 1 番目の量子ビットに作用する 1 量子ビット位相ゲートで表される. 残りの制御 $AXBXC$ ゲートは補題 5.4 で示したように, 3 個の $SU(2)$ ゲートと 2 個の CNOT ゲートで実現できる. したがって以下の分解が成り立つ (図 9) :

$$CU = (D \otimes I)(I \otimes A)\mathrm{CNOT}(I \otimes B)\mathrm{CNOT}(I \otimes C), \tag{120}$$

ただし $D = R_z(-\phi)\Phi(\phi/2)$.

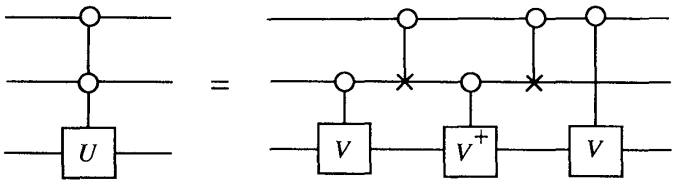
形式的には

$$\begin{aligned}
&(D \otimes I)(I \otimes A)\mathrm{CNOT}(I \otimes B)\mathrm{CNOT}(I \otimes C) \\
&= \left((|0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|) \otimes I\right)(|0\rangle\langle 0| \otimes ABC + |1\rangle\langle 1| \otimes AXBXC) \\
&= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\phi}AXBXC = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.
\end{aligned}$$

よって命題が証明された. ∎

STEP 3 (CCNOT ゲートとその変形)
最後に n 個の制御ビットをもつ制御 U ゲートも 1 量子ビットゲートと CNOT ゲートで構成できることを示そう．$n=2$ の簡単な例から調べよう．

補題 5.6 次の 2 つの量子回路 (C^2U ゲート) は等しい (ただし $U=V^2$) :



証明: 図の右側の回路を考える．第 1 第 2 量子ビットがともに 0 であれば，すべてのゲートは自明となり第 3 ビットは変換を受けない．したがってこの部分空間においてゲートは $|00\rangle\langle 00|\otimes I$ と作用する．第 1 ビットが 0 で第 2 ビットが 1 のときは第 3 ビットは $|x\rangle \mapsto V^\dagger V|x\rangle = |x\rangle$ と写像される．したがってゲートは $|01\rangle\langle 01|\otimes I$ と作用する．第 1 ビットが 1 で第 2 ビットが 0 のときは，第 3 ビットは $|x\rangle \mapsto VV^\dagger|x\rangle = |x\rangle$ となり，ゲートは $|10\rangle\langle 10|\otimes I$ と作用する．第 1，第 2 ビットがともに 1 のときは第 3 ビットは $|x\rangle \mapsto VV|x\rangle = U|x\rangle$ となり，この部分空間でゲートは $|11\rangle\langle 11|\otimes U$ となる．したがって，この図の右辺は

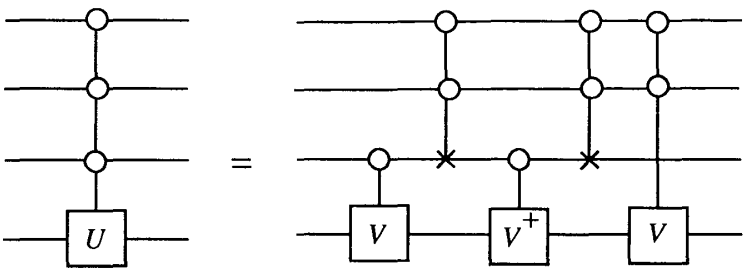
$$(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|)\otimes I + |11\rangle\langle 11|\otimes U = \mathrm{C}^2U$$

となる． ∎

この分解は直感的に以下のように解釈できる．最初の V ゲートは第 2 ビットが 1 のときのみ第 3 ビット x に作用する．$V^\dagger$ ゲートは第 1 ビット，第 2 ビットの入力 x_1, x_2 が $x_1 \oplus x_2 = x_1 + x_2 = 1 \pmod 2$ のときのみ作用する．2 番目の V ゲートは第 1 ビットが 1 のときのみ作用する．したがって第 3 ビットに対する作用は $x_1 \wedge x_2 = 1$ のときのみ $V^2 = U$ で，それ以外では I となる．

問 5.11 上の補題を右辺の各ゲートの作用をブラ，ケット，$I, U, V, V^\dagger$ を用いて具体的に書き下すことにより証明せよ．(例えば $U_{\mathrm{CNOT}} = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X$ など．)

問 5.12 図



のゲートは 3 制御ビットをつ C^3U ゲートであることを示せ．ただし $U=V^2$ である．更に多くの制御ビットをもつゲートへの一般化は明らかであろう．

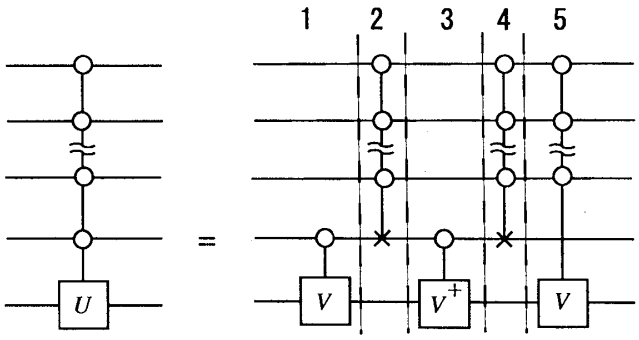


図 10: $C^{n-1}U$ ゲートの分解．一番上の数は層を表す．

命題 5.2 $n-1$ 個の制御ビットをもつ $C^{n-1}U$ ゲートは図 10 のように分解できることを示せ．
(証明は補題 5.6 と問 5.12 の証明と同様なので読者に任せる)．

その他のゲートも「基本量子ゲート」すなわち 1 量子ビットゲートと CNOT ゲートで構成できる (Barenco *et al.*)．いくつか注意をする．上のゲートは $\Theta(n^2)$ 個の基本ゲートを必要とする．[7]図 10 のゲートを実現するのに必要なゲートの数を $C(n)$ としよう．以下 $C(n)=\Theta(n^2)$ を示す．第 1 層と第 3 層の構成には n に独立な数の基本ゲートが必要である．$(n-2)$ 制御ビットをもつ制御 ${}^{(n-2)}X$ ゲートには $\Theta(n)$ 個の基本ゲートが必要であることが示される．したがって第 2 層，第 4 層には $\Theta(n)$ の基本ゲートが必要である．(Barenco *et al.* を参照) 最後に第 5 層は $C(n-1)$ 個の基本ゲートが必要である．したがって漸化式

$$C(n)-C(n-1)=\Theta(n) \tag{121}$$

が得られる．これから $C(n)=\Theta(n^2)$ が示された．

以上で U(2) ゲートと CNOT ゲートを基本量子ゲートとして用いれば，任意の n 量子ビットゲートが構成できることが示された．しかし，この構成は計算リソース，すなわちゲートの数や計算時間に関し，最適性は保障していない．デコヒーレンスやゲート操作にともなうエラーを最小にするには 9 章に示すように，これらを最適化することが望ましい．

5.5 量子並列性

典型的な量子コンピュータは入力 x にたいし関数 f が作用した結果 $f(x)$ を

$$U_f:|x\rangle|0\rangle\mapsto|x\rangle|f(x)\rangle \tag{122}$$

[7]我々物理学者は ～ のオーダーというときにあまり厳密には考えない．計算理論では 3 種類のオーダーを用いる．$n_0\in\mathbb{N}$ と $c\in\mathbb{R}$ が存在し $n\geq n_0$ のときに $f(n)\leq cg(n)$ であれば「$f(n)$ は $O(g(n))$」という．言い換えると O は $f(n)$ の漸近的な上限を示す．もし $n_0\in\mathbb{N}$ と $c\in\mathbb{R}$ が存在し $n\geq n_0$ にたいし $f(n)\geq cg(n)$ であれば「$f(n)$ は $\Omega(g(n))$」であるという．言い換えると Ω は $f(n)$ の漸近的な下限を与える．$f(n)$ が漸近的に $g(n)$ と振舞うとき，すなわち $f(n)$ が $O(g(n))$ と同時に $\Omega(g(n))$ であるとき「$f(n)$ は $\Theta(f(n))$ である」という．

のように出力する．U_f が多くの状態の線型重ね合わせ状態に作用するとしよう．U_f は線型であるから重ね合わせのメンバーすべてに作用し，出力も重ね合わせ状態となる：

$$U_f : \sum_x |x\rangle \otimes |0\rangle \mapsto \sum_x |x\rangle \otimes |f(x)\rangle. \tag{123}$$

したがって n 個の入力 $\{x_k\}$ にたいし U_f は n 個の $f(x_k)$ $(1 \leq k \leq n)$ を同時に求める．これを量子並列性といい，量子計算に指数関数的なパワーを与える．一般に式 (123) の右辺はもつれた状態であることに注意しよう．量子コンピュータは量子並列性ともつれた状態を利用できるという点で古典コンピュータにくらべ大きく優れている．

多くの量子アルゴリズムでユニタリー変換はすべての状態の重ね合わせ状態に作用する．この状態は $|00\ldots0\rangle = |0\rangle \otimes |0\rangle \otimes \ldots \otimes |0\rangle$ に Walsh-Hadamard 変換を作用させて生成できる：

$$(H \otimes H \otimes \ldots \otimes H)|00\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \tag{124}$$

すると U_f の線形性により

$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f(|x, 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle \tag{125}$$

が得られる．重ね合わせは $2^n = e^{n \ln 2}$ 状態からなり，これが古典計算に比べ量子計算を指数関数的に早くする可能性を与える．

例えばCCNOTゲートを考えよう．入力第3ビットを $|0\rangle$ に固定すると，その出力は $|x, y, x \wedge y\rangle$ となる．ただし $|x\rangle$, $|y\rangle$ は第1，第2ビットの入力である．入力がすべての可能な状態の重ね合わせとする．(ただし第3ビットは $|0\rangle$) これは Walsh-Hadamard 変換を用いて

$$H|0\rangle \otimes H|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle)$$

と生成される．CCNOT を作用させると

$$U_{\mathrm{CCNOT}}(H|0\rangle \otimes H|0\rangle \otimes |0\rangle) = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle) \tag{126}$$

が得られる．出力はCCNOTの真理値表に他ならない．出力はもつれた状態で，測定により状態は真理値表の一列に射影される．3個の量子ビットを測定する順番は問題ではない．3番目のビットの測定は，状態を測定された3番目のビットの値をもつ状態の重ね合わせに射影する．測定を繰り返すことにより状態は $|x, y, x \wedge y\rangle$ のどれか一つに収縮する．

この段階では古典コンピュータに比べ量子コンピュータの利点は何もない．測定により得られる結果はただ一つである．しかも悪いことに，特定のベクトル $|x, y, x \wedge y\rangle$ を前もって選ぶことはできない！したがって，量子アルゴリズムはある特定のベクトルが観測されるように他のベクトルに比べその係数が大きくなるようにプログラムを作成しなければならない．このステップは古典的な対比物をもたず，量子コンピュータ独特のものである．このステップを実行するためには

1. 観測したいベクトルの係数を増幅するためにその振幅を増幅する．これはGroverのデータベース検索アルゴリズムで使われている．または
2. すべてのxにたいする関数$f(x)$の共通の性質を見つける．これはShorのアルゴリズムにおいてfの周期を見つけるために量子Fourier変換の中で用いられる．

6 離散積分変換

現在Shorの素因数分解アルゴリズムとGroverのデータベース・サーチ・アルゴリズムの2つの量子アルゴリズムが古典アルゴリズムを凌駕する量子コンピュータの実用的な応用として知られている．このどちらも離散積分変換を利用している．詳しくは[3]を参照されたい．

6.1 離散積分変換

定義 6.1 $n \in \mathbb{N}$, $N \equiv 2^n$ とし，集合 $S_n = \{0, 1, \ldots, N-1\}$ を定める．ここで写像

$$K : S_n \times S_n \to \mathbb{C} \tag{127}$$

を考えよう．S_n 上の任意の複素数値関数 $f : S_n \to \mathbb{C}$ にたいし，K を核とする f の変換 $\tilde{f} : S_n \to \mathbb{C}$ を

$$\tilde{f}(y) = \sum_{x=0}^{N-1} K(y,x) f(x) \tag{128}$$

で定義する．この変換 $f \to \tilde{f}$ を**離散積分変換**という．

K の N^2 個の全ての値をまとめて，$K(x,y)$ を行列 $K \in M(N,\mathbb{C})$ の (x,y) 成分であると思ってもよい．同様に $f(x)$, $\tilde{f}(y)$ は N 成分のベクトルと思えば (128) は行列によるベクトルの変換に過ぎない．

命題 6.1 核 K はユニタリーとする; $K^\dagger = K^{-1}$. すると逆変換 $\tilde{f} \to f$ が存在し

$$f(x) = \sum_{y=0}^{N-1} K^\dagger(x,y) \tilde{f}(y). \tag{129}$$

で与えられる．

証明: (128) を (129) の右辺に代入すると

$$\begin{aligned} \sum_{y=0}^{N-1} K^\dagger(x,y)\tilde{f}(y) &= \sum_{y=0}^{N-1} K^\dagger(x,y) \left[\sum_{z=0}^{N-1} K(y,z) f(z) \right] \\ &= \sum_{y=0}^{N-1} \left[\sum_{z=0}^{N-1} K^\dagger(x,y) K(y,z) \right] f(z) = \sum_{z=0}^{N-1} \delta_{xz} f(z) = f(x). \end{aligned}$$

∎

$N=2^n$ とし U を n 量子ビット空間 $\mathcal{H}=\mathbb{C}^N$ に作用する $N\times N$ ユニタリー行列とする．$\mathcal{H}$ の標準基底を $\{|x\rangle=|x_{n-1},x_{n-2}\ldots,x_0\rangle\}$ とする．ただし $x=x_{n-1}2^{n-1}+x_{n-2}x^{n-2}+\ldots+x_02^0$. すると

$$U|x\rangle=\sum_{y=0}^{N-1}|y\rangle\langle y|U|x\rangle=\sum_{y=0}^{N-1}U(y,x)|y\rangle. \tag{130}$$

$U(x,y)=\langle x|U|y\rangle$ はこの基底における U の (x,y) 成分．

命題 6.2 U を $\mathcal{H}=\mathbb{C}^N$ に作用するユニタリー変換とする．U は

$$U|x\rangle=\sum_{y=0}^{N-1}K(y,x)|y\rangle \tag{131}$$

を満たすとする．このとき U は任意の $y\in S_n$ にたいし積分変換 $\tilde{f}(y)=\sum_{x=0}^{N-1}K(y,x)f(x)$ を

$$U\left[\sum_{x=0}^{N-1}f(x)|x\rangle\right]=\sum_{y=0}^{N-1}\tilde{f}(y)|y\rangle. \tag{132}$$

のように“計算する”．[8] ここに $|x\rangle=|x_{n-1},x_{n-2}\ldots,x_0\rangle$ などは $\mathcal{H}$ の基底である．

証明:

$$\begin{aligned}U\left[\sum_{x=0}^{N-1}f(x)|x\rangle\right] &= \sum_{x=0}^{N-1}f(x)U|x\rangle\\ &= \sum_{x=0}^{N-1}f(x)\left[\sum_{y=0}^{N-1}K(y,x)|y\rangle\right]=\sum_{y=0}^{N-1}\left[\sum_{x=0}^{N-1}K(y,x)f(x)\right]|y\rangle\\ &= \sum_{y=0}^{N-1}\tilde{f}(y)|y\rangle.\end{aligned} \tag{133}$$

∎

問 6.1

$$\sum_{x=0}^{N-1}|f(x)|^2=\sum_{y=0}^{N-1}|\tilde{f}(y)|^2 \tag{134}$$

を証明せよ．

6.2　重要な例

6.2.1　離散 Fourier 変換 (DFT)

離散積分変換の中でも最も重要なものは**離散 Fourier 変換 (DFT: Discrete Fourier Transform)** である．$\omega=e^{2\pi i/N}$ $(N=2^n)$ を 1 の N 重根とする．ω は核 $K:S_n\times S_n\to\mathbb{C}$ を

$$K(x,y)=\frac{1}{\sqrt{N}}\omega^{-xy} \tag{135}$$

[8] 命題は U が確率振幅 $f(x)$ の状態を，$f(x)$ と核 K で結ばれている確率振幅 $\tilde{f}(y)$ の状態へ写すと主張している．

で定める．この核が定義する離散積分変換

$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \omega^{-xy} f(x) \tag{136}$$

を離散 Fourier 変換 (DFT) という．K はユニタリーである：

$$\begin{aligned}(KK^\dagger)(x,y) &= \langle x|K \sum_z |z\rangle\langle z|K^\dagger|y\rangle = \sum_z K(x,z)K^\dagger(z,y) \\ &= \frac{1}{N}\sum_z e^{-xz}e^{yz} = \frac{1}{N}\sum_z \omega^{-(x-y)z} = \delta_{xy}.\end{aligned}$$

$n=1$ のとき

$$K_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & e^{2\pi i/2} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

$n=2$ のとき $\omega = e^{2\pi i/4} = i$ で

$$K_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \omega^{-3} \\ 1 & \omega^{-2} & \omega^{-4} & \omega^{-6} \\ 1 & \omega^{-3} & \omega^{-6} & \omega^{-9} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & 1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}.$$

逆 DFT は

$$f(x) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{xy} \tilde{f}(y). \tag{137}$$

重要な恒等式は

$$U|0\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle \tag{138}$$

ここに U は DFT を実現するユニタリーゲートである．この式は $f(x) = \delta_{x0}$ の DFT は $\tilde{f}(y) = 1/\sqrt{N}$ であることを示している．これは $\delta(x)$ の Fourier 変換と類似である．U を $|0\rangle$ に一回作用させただけで $\mathcal{H}$ のすべての状態を生成したことに注意せよ．

基本量子ゲートによる DFT の実装は後で詳しく紹介する．

6.2.2 Walsh-Hadamard 変換

$x_{n-1}x_{n-2}\ldots x_0$ と $y_{n-1}y_{n-2}\ldots y_0$ を x と y に対応する 2 進数とする．核 $W_n : S_n \times S_n \to \mathbb{C}$ を

$$W_n(x,y) = \frac{1}{\sqrt{N}}(-1)^{x_{n-1}y_{n-1}+x_{n-2}y_{n-2}+\ldots+x_0y_0}, \quad \forall x,y \in S_n \tag{139}$$

で定義する．離散積分変換

$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{x_{n-1}y_{n-1}+x_{n-2}y_{n-2}+\ldots+x_0y_0} f(x) \tag{140}$$

を **Walsh-Hadamard 変換**と言う．

問 6.2 W_n はユニタリーであることを示せ．逆変換 W_n^{-1} を求めよ．

問 6.3 W_1, W_2, W_3 を具体的に書き下し $W_2 = W_1 \otimes W_1$ を示せ．

$$W_n = \underbrace{W_1 \otimes W_1 \otimes \ldots \otimes W_1}_{n}. \tag{141}$$

を証明せよ．

したがって W_n は n 個の 1 量子ビットゲートで構成される．

6.2.3　選択的回転変換

核

$$K_n(x,y) = e^{i\theta_x}\delta_{xy}, \quad \forall x, y \in S_n \tag{142}$$

を定義する．ここに $\theta_x \in \mathbb{R}$ である．この離散積分変換は

$$\tilde{f}(y) = \sum_{x=0}^{N-1} K(x,y)f(x) = \sum_{x=0}^{N-1} e^{i\theta_x}\delta_{xy}f(x) = e^{i\theta_y}f(y) \tag{143}$$

である．これを**選択的回転変換 (selectively rotational transformation)** という．

問 6.4 この K_n はユニタリーであることを証明せよ．逆変換 K_n^{-1} を書き下せ．

K_1 と K_2 の行列表示は

$$K_1 = \begin{pmatrix} e^{i\theta_0} & 0 \\ 0 & e^{i\theta_1} \end{pmatrix}, K_2 = \begin{pmatrix} e^{i\theta_0} & 0 & 0 & 0 \\ 0 & e^{i\theta_1} & 0 & 0 \\ 0 & 0 & e^{i\theta_2} & 0 \\ 0 & 0 & 0 & e^{i\theta_3} \end{pmatrix}.$$

K_n は基本量子ゲートにより以下のように実現される．$n = 2$ の例を考えよう．核 K_2 は 2 つのレベル 2 のユニタリー行列で

$$K_2 = A_0A_1,\ A_0 = \begin{pmatrix} e^{i\theta_0} & 0 & 0 & 0 \\ 0 & e^{i\theta_1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\theta_2} & 0 \\ 0 & 0 & 0 & e^{i\theta_3} \end{pmatrix} \tag{144}$$

と分解できる．恒等式

$$A_1 = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U_1, \quad U_1 = \begin{pmatrix} e^{i\theta_2} & 0 \\ 0 & e^{i\theta_3} \end{pmatrix} \tag{145}$$

に注意せよ．したがって A_1 は制御 U ゲートである．A_0 に関しては，まず第 1 ビットの否定を取って左上のブロックと右下のブロックを交換する；

$$|0\rangle = |00\rangle \to |10\rangle = |3\rangle, |1\rangle = |01\rangle \to |11\rangle = |4\rangle, |2\rangle = |10\rangle \to |00\rangle = |0\rangle, |3\rangle = |11\rangle \to |01\rangle = |1\rangle.$$

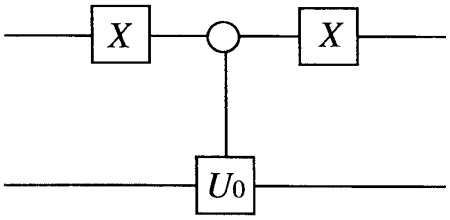


図 11: 基本量子ゲートを用いた A_0 の実現.

それから制御 U_0 ゲート，ただし

$$U_0 = \begin{pmatrix} e^{i\theta_0} & 0 \\ 0 & e^{i\theta_1} \end{pmatrix}$$

を行い，その後第 1 ビットの否定を取る．したがって A_0 は図 11 のように表される．実際，このゲートは具体的に

$$\begin{aligned} & (X \otimes I)(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U_0)(X \otimes I) \\ &= X|0\rangle\langle 0|X \otimes I + X|1\rangle\langle 1|X \otimes U_0 = |1\rangle\langle 1| \otimes I + |0\rangle\langle 0| \otimes U_0 \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes I + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes U_0 \\ &= \begin{pmatrix} e^{i\theta_0} & 0 & 0 & 0 \\ 0 & e^{i\theta_1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{aligned} \tag{146}$$

とかかれる．したがってこのゲートは基本量子ゲートで実現できる．

問 6.5 $n = 3$ の場合に上の議論を繰り返せ．K_3 は 4 個のレベル 2 のユニタリー行列の積で書ける．これらの行列を書き下しこれらの行列を実現する量子回路を求めよ．

6.3 DFT の量子回路

DFT を実現する量子回路 U を求めよう．U は状態 $\sum_x f(x)|x\rangle$ を $\sum_y \tilde{f}(y)|y\rangle$ へ写像する．ここに

$$\tilde{f}(y) = \frac{1}{\sqrt{N}} \sum_x \omega^{-xy} f(x), \quad \omega = e^{2\pi i/N}, N = 2^n$$

である．したがって

$$U|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{2^n-1} e^{-2\pi i xy/N} |y\rangle.$$

まず $n = 1, 2, 3$ の DFT を考えよう．

$\underline{n = 1}$

$n=1$ の DFT は

$$\tilde{f}(y)=\frac{1}{\sqrt{2}}\sum_{x=0}^{1}\omega^{-xy}f(y)=\frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{xy}f(y). \tag{147}$$

である．$n=1$DFT を実現する量子回路 $U^{(1)}$ は

$$\begin{aligned}U^{(1)}|x\rangle &= \frac{1}{\sqrt{2}}\sum_{y=0}^{1}\omega^{-xy}|y\rangle=\frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{-xy}|y\rangle \\ &= \sum_{y=0}^{1}\frac{1}{\sqrt{2}}(-1)^{xy}|y\rangle\end{aligned} \tag{148}$$

を満たす．

一方，Haramard ゲート H の $|x\rangle$ への作用は

$$H|x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+(-1)^{x}|1\rangle)=\frac{1}{\sqrt{2}}\sum_{y=0}^{1}(-1)^{xy}|y\rangle. \tag{149}$$

これは $n=1$DFT ゲートは Hadamard ゲートに等しいことを示している．実際 $|\psi\rangle=f(0)|0\rangle+f(1)|1\rangle$ を 1 量子ビット状態としよう．すると

$$\begin{aligned}H|\psi\rangle &= f(0)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)+f(1)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\ &= \frac{1}{\sqrt{2}}\left(f(0)+f(1)\right)|0\rangle+\frac{1}{\sqrt{2}}\left(f(0)-f(1)\right)|1\rangle,\end{aligned} \tag{150}$$

となり $n=1$DFT と同じ結果が得られた．

$\underline{n=2}$

制御 B_{jk} ゲートを導入しよう．B_{jk} は行列

$$B_{jk}=\begin{pmatrix}1 & 0\\ 0 & e^{-i\theta_{jk}}\end{pmatrix},\quad \theta_{jk}=\frac{2\pi}{2^{k-j+1}}\ (j,k\in\mathbb{N}) \tag{151}$$

で定義される．

補題 6.1 図 12 の制御 B_{jk} ゲート U は $|x,y\rangle$ $(x,y\in\{0,1\})$ に

$$U|x,y\rangle=e^{-i\theta_{jk}xy}|x,y\rangle=\exp\left(-\frac{2\pi i}{2^{k-j+1}}xy\right)|x,y\rangle \tag{152}$$

と作用する．

証明: 制御 B_{jk} ゲート $U_{jk}=|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes B_{jk}$ の $|x,y\rangle$ への作用は

$$\begin{aligned}U_{jk}|x,y\rangle &= |0\rangle\langle 0|x\rangle\otimes|y\rangle+|1\rangle\langle 1|x\rangle\otimes B_{jk}|y\rangle \\ &= \begin{cases}|x\rangle\otimes|y\rangle & x=0\\ |x\rangle\otimes B_{jk}|y\rangle & x=1\end{cases}\end{aligned} \tag{153}$$

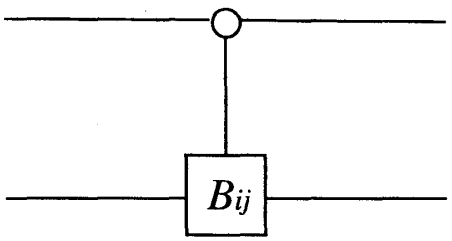


図 12: 制御 B_{ij} ゲート.

となる. さらに $x=1$ のとき

$$B_{jk}|y\rangle = \begin{cases} |y\rangle & y=0 \\ e^{-i\theta_{jk}}|y\rangle & y=1 \end{cases} \tag{154}$$

これらの結果をまとめると (152) となる. ∎

$n=2$ の DFT は

$$\tilde{f}(y) = \frac{1}{\sqrt{2^2}} \sum_{x=0}^{3} \omega^{-xy} f(x), \quad \omega = e^{2\pi i/4} = i, \ y \in S_2 = \{0,1,2,3\} \tag{155}$$

我々の目的は DFT の定義により

$$U^{(2)}|x\rangle = \frac{1}{\sqrt{2^2}} \sum_{y=0}^{3} \omega^{-xy}|y\rangle. \tag{156}$$

を満たすユニタリー行列 $U^{(2)}$ を探すことである. x と y を 2 進数で $x = 2x_1 + x_0$ および $y = 2y_1 + y_0$ と表す. $U^{(2)}$ の $|x\rangle$ への作用は

$$\begin{aligned} U^{(2)}|x_1,x_0\rangle &= \frac{1}{\sqrt{2^2}} \sum_{y=0}^{3} e^{-2\pi i xy/2^2}|y\rangle = \frac{1}{\sqrt{2^2}} \sum_{y_0,y_1=0}^{1} e^{-2\pi i x(2y_1+y_0)/2^2}|y_1,y_0\rangle \\ &= \frac{1}{\sqrt{2^2}} \sum_{y_0,y_1} e^{-2\pi i x y_1/2}|y_1\rangle \otimes e^{-2\pi i x y_0/2^2}|y_0\rangle \\ &= \frac{1}{\sqrt{2^2}} \sum_{y_1} e^{-2\pi i x y_1/2}|y_1\rangle \otimes \sum_{y_0} e^{-2\pi i x y_0/2^2}|y_0\rangle \\ &= \frac{1}{\sqrt{2^2}} \left(|0\rangle + e^{-2\pi i x/2}|1\rangle\right) \otimes \left(|0\rangle + e^{-2\pi i x/2^2}|1\rangle\right) \\ &= \frac{1}{\sqrt{2^2}} \left(|0\rangle + e^{-2\pi i (2x_1+x_0)/2}|1\rangle\right) \otimes \left(|0\rangle + e^{-2\pi i (2x_1+x_0)/2^2}|1\rangle\right) \\ &= \frac{1}{\sqrt{2^2}} \left(|0\rangle + (-1)^{x_0}|1\rangle\right) \otimes B_{12}^{x_0} \left(|0\rangle + (-1)^{x_1}|1\rangle\right). \end{aligned} \tag{157}$$

最後の式から $n=2$ の DFT は Hadamard ゲートと U_{12} で構成されることが分かる. これを実現する量子回路を書き下す前に, 第 1 ビットは冪 $(-1)^{x_0}$ をもち, 第 2 ビットは $(-1)^{x_1}$ をもつこと

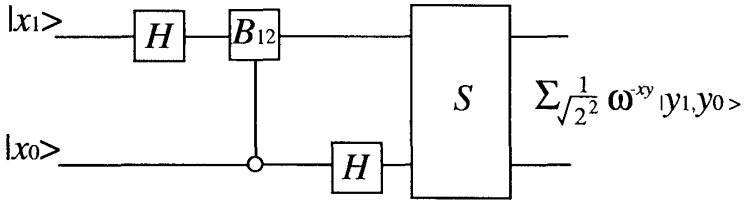


図 13: $n=2$ DFT の量子回路.

に注意しよう．もし第2ビットにナイーヴに Hadamard ゲートを作用させると

$$(I\otimes H)|x_1,x_0\rangle = |x_1\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle+(-1)^{x_0}|1\rangle)$$

となってしまう．したがって最後に第1，第2ビットを SWAP させて

$$\begin{aligned} U^{(2)}|x_1,x_0\rangle &= S\,[B_{12}^{x_0}(|0\rangle+(-1)^{x_1}|1\rangle\otimes(|0\rangle+(-1)^{x_0}|1\rangle)]. \\ &= S(I\otimes H)U_{12}(H\otimes I)|x_1,x_0\rangle \end{aligned} \tag{158}$$

としなければならない．$B_{12}^{x_0}$ の中の指数 x_0 は入力の $|x_0\rangle$ であり，$(I\otimes H)$ が $|x_0\rangle$ に作用する前の値でなければならない．以上で次の命題が証明された．

命題 6.3 $n=2$ の DFT ゲートは

$$U^{(2)} = S(I\otimes H)U_{12}(H\otimes I) \tag{159}$$

で構成される（図 13）.

問 6.6 上の命題を直接書き下すことにより $n=2$ DFT を与える 4×4 ユニタリー行列を導け.

<u>$n\geq 3$</u>

$n=2$ の結果を一般化しやすい形に書き換える．状態 $|x_1,x_0\rangle$ は

$$\begin{aligned} |x_1,x_0\rangle &\to \frac{1}{\sqrt{2^2}}\sum_{y=0}^{2^2-1}e^{-2\pi ixy/2^2}|y\rangle \\ &= \frac{1}{\sqrt{2^2}}\sum_{y_1,y_0=0}^{1}e^{-2\pi ix(y_1/2+y_0/2^2)}|y_1,y_0\rangle \\ &= \frac{1}{\sqrt{2^2}}\sum_{y_1,y_0}e^{-2\pi ixy_1/2}|y_1\rangle\otimes e^{-2\pi ixy_0/2^2}|y_0\rangle \\ &= \frac{1}{\sqrt{2^2}}(|0\rangle+e^{-2\pi ix_0/2}|1\rangle)\otimes(|0\rangle+e^{-2\pi i(x_1/2+x_0/2^2)}|1\rangle) \end{aligned} \tag{160}$$

と変換された．これから $n=3$ にたいし

$$\begin{aligned} U^{(3)}|x_2,x_1,x_0\rangle &= \frac{1}{\sqrt{2^3}}(|0\rangle+e^{-2\pi ix_0/2}|1\rangle)\otimes(|0\rangle+e^{-2\pi i(x_1/2+x_0/2^2)}|1\rangle) \\ &\quad\otimes(|0\rangle+e^{-2\pi i(x_2/2+x_1/2^2+x_0/2^3)}|1\rangle) \end{aligned} \tag{161}$$

が推測される.

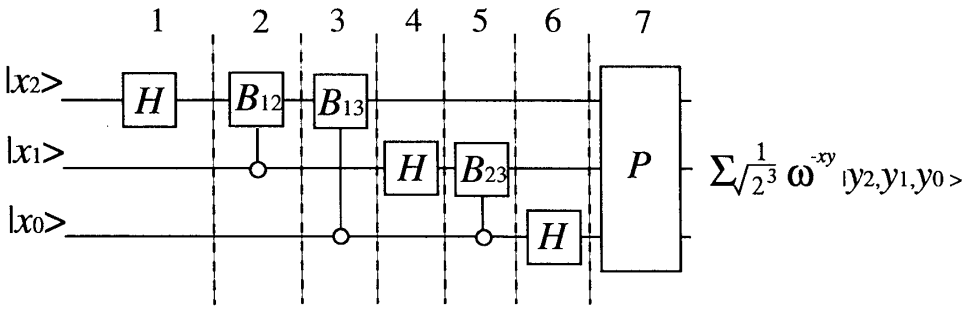


図 14: $n = 3$ DFT の量子回路.

問 6.7 $x = 2^2x_2 + 2x_1 + x_0$ と $y = 2^2y_2 + 2y_1 + y_0$ とする.
(1)

$$U^{(3)}|x_2, x_1, x_0\rangle = \frac{1}{\sqrt{2^3}} \sum_{y=0}^{2^3-1} e^{-2\pi i xy/2^3}|y\rangle \tag{162}$$

の右辺を x_i と y_i で具体的に書き下せ.
(2) (161) の右辺は (162) と一致することを示せ.

$n = 2$ DFT の量子回路を真似すると $n = 3$ にたいして図 14 が得られる. ここにゲート P はビットの順番を逆転するゲート :

$$P|x_2, x_1, x_0\rangle = |x_0, x_1, x_2\rangle. \tag{163}$$

問 6.8 P を表す 8×8 行列を書き下せ.

問 6.9 図 14 は実際 $n = 3$ DFT であることを示せ.

したがって次の命題が証明された.

命題 6.4 $n = 3$ DFT を表すユニタリーゲート $U^{(3)}$ は (図 14)

$$U^{(3)} = P(I \otimes I \otimes H)U_{23}(I \otimes H \otimes I)U_{13}U_{12}(H \otimes I \otimes I) \tag{164}$$

で与えられる。

問 6.10 式 (164) の右辺を書き下し, これが $n = 3$ DFT を表すユニタリー行列 U であることを示せ.

$n \geq 4$ への一般化はほとんど自明である. (161) の一般化は

$$\begin{aligned} & U^{(n)}|x_{n-1}, \ldots, x_1, x_0\rangle \\ &= \frac{1}{\sqrt{2^n}}(|0\rangle + e^{-2\pi i x_0/2}|1\rangle) \otimes (|0\rangle + e^{-2\pi i(x_1/2 + x_0/2^2)}|1\rangle) \\ &\quad \otimes (|0\rangle + e^{-2\pi i(x_2/2 + x_1/2^2 + x_0/2^3)}|1\rangle) \otimes \ldots \\ &\quad \ldots \otimes (|0\rangle + e^{-2\pi i(x_{n-1}/2 + x_{n-2}/2^2 + \ldots x_1/2^{n-1} + x_0/2^n)}|1\rangle) \end{aligned} \tag{165}$$

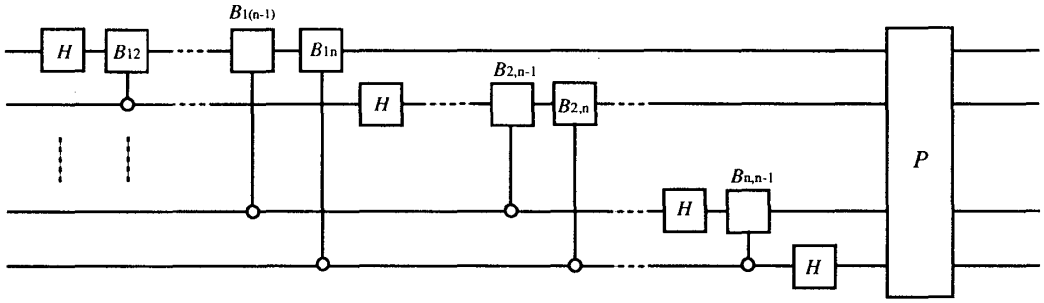


図 15: n 量子ビット DFT の量子回路.

である．図 15 の回路が実際 n 量子ビット DFT であることは，例えば帰納法で証明される．

問 6.11 式 (165) が n 量子ビット DFT であることを示せ.

命題 6.5 n 量子ビット DFT は $\Theta(n^2)$ の基本ゲートで構成される.

証明: n-qubit DFT は 1 つの P ゲート, n 個の Hadamard gates および $(n-1)+(n-2)+\ldots+2+1 = n(n-1)/2$ 個の制御 B_{jk} ゲートで構成される（図 15）問 4.5 (3) と §5.2.4 で示されたように SWAP ゲートは 3 個の CNOT ゲートで構成される．さらに n 量子ビットの P ゲートは $\sim n/2$ 個の SWAP ゲートを必要とする[9]．したがって P ゲートは $3 \times [n/2] = \Theta(n)$ の基本ゲートからなる．命題 5.1 により制御 B_{ij} gate は高々 6 個の基本ゲートから構成される．したがって n 量子ビット DFT は $\Theta(n^2)$ の基本ゲートから構成される. ∎

上の命題は量子アルゴリズムの複雑さを見積もる上で大変重要である．定義

$$\tilde{f}(y) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \omega^{-xy} f(x)$$

を眺めるとナイーヴには，各 y にたいし 2^n ステップが必要で，全ての y では $2^n \times 2^n$ ステップすなわち，指数関数的に多くのステップ ($\sim 2^{2n \ln 2}$) が必要となる．上の命題は量子 DFT では，初期状態がすべての x の重ね合わせであれば多項式ステップ $\Theta(n^2)$ でこれが実行できることを主張している．より詳しくは，例えば [3] を参照されたい．Shor のアルゴリズムでは DFT が重要な役割を果たし，そのために古典的には n の指数関数時間かかる計算が多項式時間で実行できる.

6.4 DFT の応用

後で使われる量子 DFT の応用を先取りする．2 個のレジスター |REG1⟩ と |REG2⟩ からなる系を考える．例えば，各レジスターは 3 量子ビット系とし，全系は |REG1⟩ ⊗ |REG2⟩ であるとする．|REG1⟩ の初期状態を

$$\frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + \ldots + |111\rangle) = \frac{1}{\sqrt{8}}(|0\rangle + |1\rangle + \ldots + |7\rangle). \tag{166}$$

[9]正確にいえば $[n/2]$ 個の SWAP ゲートである.

とし，ある関数 f を作用させ

$$|\Psi\rangle = U_f \frac{1}{\sqrt{8}} \sum_x |x\rangle|0\rangle = \frac{1}{\sqrt{8}} \sum_x |x, f(x)\rangle = \frac{1}{\sqrt{8}}(|0, f(0)\rangle + \ldots + |7, f(7)\rangle) \tag{167}$$

を得る．$|\Psi\rangle$ に含まれるベクトルは $|k, f(k)\rangle$ の対角形であり，その位相はすべて 1 であることに注意されたい．

次に第 1 レジスターに $n = 3$ DFT $U^{(3)}$ を施す．

$$|x\rangle \to \frac{1}{\sqrt{8}} \sum_{y=0}^{7} e^{-2\pi i x y/8} |y\rangle. \tag{168}$$

すると

$$\begin{aligned}
|\Psi'\rangle &= U^{(3)}|\Psi\rangle = \frac{1}{8} \sum_{x,y} e^{-2\pi i x y/8} |y, f(x)\rangle \\
&= \frac{1}{8}|0\rangle \otimes [|f(0)\rangle + |f(1)\rangle + \ldots + |f(7)\rangle] \ (y = 0) \\
&\quad + \frac{1}{8}|1\rangle \otimes \left[|f(0)\rangle + e^{-2\pi i/8}|f(1)\rangle + \ldots + e^{-2\pi i 7/8}|f(7)\rangle\right] \quad (y = 1) \\
&\quad \cdots \\
&\quad + \frac{1}{8}|7\rangle \otimes \left[|f(0)\rangle + e^{-14\pi i/8}|f(1)\rangle + \ldots + e^{-14\pi i 7/8}|f(7)\rangle\right]. \quad (y = 7)
\end{aligned} \tag{169}$$

が得られる．$|\Psi'\rangle$ にはすべての $|j, f(k)\rangle$ が含まれていることに注意せよ．またさまざまな位相が現れている．式 (169) は第 1 レジスターの状態によって因数分解した形に書かれている．

ここで $f(x)$ は $f(x + P) = f(x)$ を満たす周期関数であるとする．ただし $P \in \mathbb{N}$．この周期は $|\mathrm{REG1}\rangle$ を観測すれば分かる．たとえば $P = 2$ とすると

$$f(0) = f(2) = f(4) = f(6), \quad f(1) = f(3) = f(5) = f(7).$$

すると状態 $|\Psi'\rangle$ は

$$\begin{aligned}
|\Psi'\rangle &= \frac{1}{8} \sum_{x,y} e^{-2\pi i x y/8} |y, f(x)\rangle \\
&= \frac{1}{2}|0\rangle \otimes [|f(0)\rangle + |f(1)\rangle] \\
&\quad + \frac{1}{8}|1\rangle \otimes \left[|f(0)\rangle \left(1 + e^{-1\cdot 2\cdot 2\pi i/8} + e^{-1\cdot 4\cdot 2\pi i/8} + e^{-1\cdot 6\cdot 2\pi i/8}\right)\right. \\
&\quad \left. + |f(1)\rangle \left(e^{-1\cdot 1\cdot 2\pi i/8} + e^{-1\cdot 3\cdot 2\pi i/8} e^{-1\cdot 5\cdot 2\pi i/8} + e^{-1\cdot 7\cdot 2\pi i/8}\right)\right] \\
&\quad \cdots
\end{aligned} \tag{170}$$

と表される．したがって

$$|0, f(0)\rangle, |0, f(1)\rangle, |4, f(0)\rangle, |4, f(1)\rangle$$

を除くすべてのベクトルはキャンセルしてしまい

$$|\Psi'\rangle = \frac{1}{2}\left(|0, f(0)\rangle + |0, f(1)\rangle + |4, f(0)\rangle + e^{-i\pi}|4, f(1)\rangle\right) \tag{171}$$

となる．したがって $|\mathrm{REG1}\rangle$ を測定すると，結果は 0 または 4 となりこれから $P = 2$ が推察される．

問 6.12 各レジスターは n 量子ビット系であるとする．$f(x)$ は周期 P の周期関数であるとする．ただし 2^n は P で割り切れるとする．1 番目のレジスターに n 量子ビット DFT を作用させた後の観測値は以下のどれかであることを示せ：

$$0, \frac{1\cdot 2^n}{P}, \frac{2\cdot 2^n}{P}, \frac{3\cdot 2^n}{P}, \ldots, \frac{(P-1)2^n}{P}. \tag{172}$$

この位相のキャンセレーションは Shor のアルゴリズムで中心的な役割を果たす．

7　Grover のデータベース検索アルゴリズム

ランダムに並べられた N 個のファイルがあり，その中のある条件を満たす一つまたは複数の特定のファイルを取り出したいとする．これはデータベース検索問題といわれる．ここで対象とするのは構造をもたないデータベースである．たとえば電話帳は名前の順に並んでいるという構造をもっており，名前からその人の電話番号を検索するのはたやすい．一方，電話帳の番号は構造をもっておらず，電話番号からその持ち主を探すのは困難である．このような場合古典的アルゴリズムでは，ファイルをしらみつぶしに探すことになり，それには $O(N)$ ステップの手続きが必要となる．この問題は量子アルゴリズムを使うと $O(\sqrt{N})$ ステップで検索できることは Grover が最初に発見した [9, 10].

7.1　一つのファイルの検索

ランダムに並べられた $N = 2^n$ 件のファイルがあるとしよう．集合 $S_n \equiv \{x \in \mathbb{Z} | 0 \le x \le N-1\}$ を定義し，各ファイルには $x \in S_n$ のアドレスが与えられているとする．以下では，ある条件を満たす特定のファイルを検索するアルゴリズムを考える．

数学的な言葉を使うと，これは以下のように表される．関数 $f : S_n \to \{0, 1\}$ は

$$f(x) = \begin{cases} 1 & (x = z) \\ 0 & (x \neq z) \end{cases} \tag{173}$$

で定義される関数とする．ただし z は我々が探そうするファイルのアドレスである．関数 $f(x)$ は直ちに計算され，そのための計算ステップは無視することができると仮定する．このような関数は「**オラクル (oracle)**」と言われる．結局，問題は 1 点でのみ 1 をとる関数 $f : S_n \to \{0, 1\}$ が与えられたとき，$f(z) = 1$ となる点 z を求めることに帰着する．

古典的には各ファイルを次々にチェックし，$f(z)=1$ となる z を探さなければならないので $O(N)$ のステップが必要となる．Grover が示したように，量子アルゴリズムでは $O(\sqrt{N})$ のステップでこのファイルが検索できるものが存在する．このアルゴリズムは $|z\rangle$ の振幅を増幅し，他のベクトル $|x\rangle$ $(x \neq z)$ の振幅はキャンセルするように作用する．

Grover のアルゴリズムは以下のステップに分けられる．

STEP 1 (選択的回転変換)

選択的回転変換の核を

$$R_f(x,y) = e^{i\pi f(x)}\delta_{xy} = (-1)^{f(x)}\delta_{xy} \qquad (x,y \in S_n) \tag{174}$$

で定義する．R_f は $|z\rangle \to -|z\rangle$ と写像するが，それ以外のすべての基底ベクトル $|x\rangle$ は不変とするので，

$$R_f = I - 2|z\rangle\langle z| \tag{175}$$

と表すこともできる．

状態 $|\varphi\rangle$ を

$$|\varphi\rangle = \sum_{x=0}^{N-1} w_x|x\rangle, \quad \sum_x |w_x|^2 = 1 \tag{176}$$

で定義すると

$$\begin{aligned} R_f|\varphi\rangle &= (I - 2|z\rangle\langle z|)\sum_{x=0}^{N-1} w_x|x\rangle = \sum_{x=0}^{N-1} w_x|x\rangle - 2w_z|z\rangle \\ &= w_0|0\rangle + \ldots + (-1)w_z|z\rangle + \ldots + w_{N-1}|N-1\rangle = \sum_{x\neq z} w_z|x\rangle - w_z|z\rangle \end{aligned} \tag{177}$$

が成り立つ．すなわち R_f は w_z の符号を反転するだけで他の成分は不変に保つ．

STEP 2 次に W を Walsh-Hadamard 変換

$$W(x,y) = \frac{1}{\sqrt{2^n}}(-1)^{x_{n-1}y_{n-1}+\ldots+x_1y_1+x_0y_0}, \quad (x,y \in S_n) \tag{178}$$

R を選択的回転変換

$$R(x,y) = e^{i\pi(1-\delta_{x0})} = (-1)^{1-\delta_{x0}}\delta_{xy} \tag{179}$$

として，ユニタリー行列

$$D = WRW \tag{180}$$

を定義する．

命題 7.1 状態 $|\varphi_0\rangle$ を

$$|\varphi_0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle \tag{181}$$

で定義すると

$$D = -I + 2|\varphi_0\rangle\langle\varphi_0| \tag{182}$$

となる．さらに $|\varphi\rangle$ を式 (176) で与えると

$$D|\varphi\rangle = \sum_{x=0}^{2^n-1} (\bar{w} - (w_x - \bar{w}))\,|x\rangle, \tag{183}$$

が成り立つ．ここに

$$\bar{w} = \frac{1}{2^n}\sum_{x=0}^{2^n-1} w_x \tag{184}$$

は w_x の平均値．

証明: 式 (182) の右辺を求めよう．等式

$$-I + 2|\varphi_0\rangle\langle\varphi_0| = -I + \frac{2}{2^n}\sum_x |x\rangle \sum_y \langle y| = -I + \frac{2}{2^n}\sum_{x,y} |x\rangle\langle y|$$

から，右辺の (x,y) 成分は

$$\langle x|\mathrm{RHS}|y\rangle = -\delta_{xy} + \frac{2}{N}$$

となる．

次に左辺を調べよう．$D = WRW$ の (x,y) 成分は

$$\begin{aligned}\langle x|WRW|y\rangle &= \sum_{u,v}\langle x|W|u\rangle\langle u|R|v\rangle\langle v|W|v\rangle \\ &= \frac{1}{\sqrt{N}}\sum_{u,v}(-1)^{x_{n-1}u_{n-1}+\ldots+x_1u_1+x_0u_0} \\ &\quad\times(-1)^{1-\delta_{u0}}\delta_{uv}(-1)^{v_{n-1}y_{n-1}+\ldots+v_1y_1+v_0y_0}.\end{aligned}$$

となる，u に関する和を実行すると

$$\begin{aligned}&\sum_{u=0}^{N-1}(-1)^{x_{n-1}u_{n-1}+\ldots+x_1u_1+x_0u_0}(-1)^{1-\delta_{u0}}\delta_{uv} \\ &= (-1)^0(-1)^0\delta_{0v} - \sum_{u=1}^{N-1}(-1)^{x_{n-1}u_{n-1}+\ldots+x_1u_1+x_0u_0}\delta_{uv} \\ &= 2\delta_{0v} - \sum_{u=0}^{N-1}(-1)^{x_{n-1}u_{n-1}+\ldots+x_1u_1+x_0u_0}\delta_{u_{n-1}v_{n-1}}\cdots\delta_{u_1v_1}\delta_{u_0v_0} \\ &= 2\delta_{0v} - \left(\sum_{u_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}}\right)\cdots\left(\sum_{u_1=0}^{1}(-1)^{x_1u_1}\right)\left(\sum_{u_0=0}^{1}(-1)^{x_0u_0}\right)\end{aligned}$$

となる．右辺は

$$\begin{aligned}D(x,y) &= \frac{1}{N}\sum_{v=0}^{N-1}\left[2\delta_{0v} - \left(\sum_{u_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}}\delta_{u_{n-1}v_{n-1}}\right)\right. \\ &\quad\left.\cdots\left(\sum_{u_0=0}^{1}(-1)^{x_0u_0}\delta_{u_0v_0}\right)\right](-1)^{v_{n-1}y_{n-1}+\ldots+v_1y_1+v_0y_0}\end{aligned}$$

$$
\begin{aligned}
&= \frac{2}{N} - \frac{1}{N}\left[\sum_{u_{n-1},v_{n-1}=0}^{1}(-1)^{x_{n-1}u_{n-1}+v_{n-1}y_{n-1}}\delta_{u_{n-1}v_{n-1}}\right] \\
&\quad \cdots\left[\sum_{u_0,v_0=0}^{1}(-1)^{x_0u_0+v_0y_0}\delta_{u_0v_0}\right] \\
&= \frac{2}{N} - \frac{1}{N}\left[1+(-1)^{x_{n-1}+y_{n-1}}\right]\cdots\left[1+(-1)^{x_0+y_0}\right] \\
&= \frac{2}{N} - \frac{1}{N}\delta_{x_{n-1}y_{n-1}}\cdots\delta_{x_0y_0} \\
&= \frac{2}{N} - \frac{1}{N}\delta_{xy}
\end{aligned}
$$

となり (182) が示された.

次に

$$
\begin{aligned}
D|\varphi\rangle &= (-I+2|\varphi_0\rangle\langle\varphi_0|)|\phi\rangle = \left(-I+\frac{2}{N}\sum_{y,z}|y\rangle\langle z|\right)\sum_x w_x|x\rangle \\
&= -\sum_x w_x|x\rangle + \frac{2}{N}\sum_{x,y,z} w_x|y\rangle\delta_{xz} = -\sum_x w_x|x\rangle + \frac{2}{N}\sum_{y,z} w_z|y\rangle \\
&= -\sum_x w_x|x\rangle + 2\sum_y \bar{w}|y\rangle = \sum_{x=0}^{N-1}\left[\bar{w}-(w_x-\bar{w})\right]|x\rangle
\end{aligned}
$$

により (183) が示された. ∎

式 (183) は D が「平均値に関する反転」を生成する演算子であることを示している：新しい確率振幅 $\bar{w}-(w_x-\bar{w})=2\bar{w}-w_x$ は w_x を $\bar{w}$ に関して反転して得られるからである.

STEP 3 次にユニタリー変換

$$
U_f = DR_f = (-I+2|\varphi_0\rangle\langle\varphi_0|)\,(I-2|z\rangle\langle z|) \tag{185}
$$

を定義し，その $|\varphi\rangle$ への作用を考えよう. STEP1 と STEP2 の結果を用いるとただちに

$$
\begin{aligned}
U_f|\varphi\rangle &= D\left(\sum_{x\neq z} w_x|x\rangle - w_z|z\rangle\right) = \sum_{x\neq z}[\bar{w}-(w_x-\bar{w})]|x\rangle + [\bar{w}+(w_z+\bar{w})]|z\rangle \\
&= \sum_{\substack{x=0\\x\neq z}}^{N-1}(2\bar{w}-w_x)|x\rangle + (2\bar{w}+w_z)|z\rangle
\end{aligned} \tag{186}
$$

が得られる. ただし $\bar{w}$ は平均値

$$
\bar{w} = \frac{1}{N}\left(\sum_{\substack{x=0\\x\neq z}}^{N-1} w_x - w_z\right) \tag{187}
$$

である.

これはすべての振幅 w_x が正のとき，U_f の作用により $|z\rangle$ の振幅は増加するが，$|x\rangle$ $(x \neq z)$ は減少することを示している．したがって，U_f を繰り返し $|\varphi\rangle$ に作用させることにより $|z\rangle$ の振幅は増加し，あるところでその振幅が 1 に近くなり，その状態で系の観測を行うと 1 に近い確率で $|z\rangle$ が観測されることになる．U_f が $|\varphi\rangle$ に k 回作用したときの状態を求めよう．

命題 7.2 $U_f^k|z\rangle$ を

$$U_f^k|\varphi_0\rangle = a_k|z\rangle + b_k \sum_{x\neq z}|x\rangle \tag{188}$$

と書く．ただし

$$a_0 = b_0 = \frac{1}{\sqrt{N}}$$

である．このとき $k = 1, 2, \ldots$ にたいし

$$a_k = \frac{N-2}{N}a_{k-1} + \frac{2(N-1)}{N}b_{k-1}, \tag{189}$$

$$b_k = -\frac{2}{N}a_{k-1} + \frac{N-2}{N}b_{k-1} \tag{190}$$

が成り立つ．

証明 帰納法で証明する．$k = 1$ のときは

$$\begin{aligned}
U_f|\varphi_0\rangle &= (-I + 2|\varphi_0\rangle\langle\varphi_0|)(I - 2|z\rangle\langle z|)\frac{1}{\sqrt{N}}\sum_x |x\rangle \\
&= (-I + 2|\varphi_0\rangle\langle\varphi_0|)\left(|\varphi_0\rangle - \frac{2}{\sqrt{N}}|z\rangle\right) \\
&= -|\varphi_0\rangle + 2|\varphi_0\rangle + \frac{2}{\sqrt{N}}|z\rangle - \frac{4}{N}|\varphi_0\rangle \\
&= \frac{1}{\sqrt{N}}\left(1 - \frac{4}{N}\right)\sum_{x\neq z}|x\rangle + \frac{1}{\sqrt{N}}\left(3 - \frac{4}{N}\right)|z\rangle \\
&= b_1 \sum_{x\neq z}|x\rangle + a_1|z\rangle.
\end{aligned}$$

よって成立．

k のとき $U_f^k|\varphi_0\rangle = a_k|z\rangle + b_k\sum_{x\neq z}|x\rangle$ が成り立つとする．このとき

$$\begin{aligned}
U_f^{k+1}|\varphi_0\rangle &= U_f U_f^k|\varphi_0\rangle = U_f(a_k|z\rangle + b_k\sum_{x\neq z}|x\rangle) \\
&= (-I + 2|\varphi_0\rangle\langle\varphi_0|)(1 - 2|z\rangle\langle z|)\left(a_k|z\rangle + b_k\sum_{x\neq z}|x\rangle\right) \\
&= (-I + 2|\varphi_0\rangle\langle\varphi_0|)(-a_k|z\rangle + b_k\sum_{x\neq z}|x\rangle) \\
&= -b_k\sum_{x\neq z}|x\rangle + a_k|z\rangle + \frac{2}{\sqrt{N}}(N-1)b_k|\varphi_0\rangle - \frac{2a_k}{\sqrt{N}}|\varphi_0\rangle \\
&= -b_k\sum_{x\neq z}|x\rangle + a_k|z\rangle + \frac{2(N-1)}{N}b_k\sum_x|x\rangle - \frac{2a_k}{N}\sum_x|x\rangle
\end{aligned}$$

$$= \left[\frac{N-2}{N}a_k + \frac{2(N-1)}{N}b_k\right]|z\rangle + \left[-\frac{2}{N}a_k + \frac{N-2}{N}b_k\right]\sum_{x\neq z}|x\rangle.$$

よって証明された. ∎

命題 7.3 $k = 1, 2, \ldots$ にたいし，命題 7.2 の係数を具体的に表すと

$$a_k = \sin[(2k+1)\theta], \quad b_k = \frac{1}{\sqrt{N-1}}\cos[(2k+1)\theta], \tag{191}$$

となる. ただし

$$\sin\theta = \sqrt{\frac{1}{N}}, \quad \cos\theta = \sqrt{1-\frac{1}{N}}. \tag{192}$$

証明 $c_k = \sqrt{N-1}b_k$ とすると，漸化式 (189) と (190) は

$$\begin{pmatrix} a_k \\ c_k \end{pmatrix} = M\begin{pmatrix} a_{k-1} \\ c_{k-1} \end{pmatrix}$$

と書かれる. ただし

$$M = \begin{pmatrix} (N-2)/N & 2\sqrt{N-1}/N \\ -2\sqrt{N-1}/N & (N-2)/N \end{pmatrix} = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}.$$

これは角度 2θ の回転行列である. したがって

$$\begin{pmatrix} a_k \\ c_k \end{pmatrix} = M^k\begin{pmatrix} a_0 \\ c_0 \end{pmatrix} = \begin{pmatrix} \cos 2k\theta & \sin 2k\theta \\ -\sin 2k\theta & \cos 2k\theta \end{pmatrix}\begin{pmatrix} \sin\theta \\ \cos\theta \end{pmatrix} = \begin{pmatrix} \sin[(2k+1)\theta] \\ \cos[(2k+1)\theta] \end{pmatrix}$$

が得られた. c_k を b_k で表せばただちに (191) が示される. ∎

したがって U_f を $|\varphi_0\rangle$ に k 回作用させると

$$U_f^k|\varphi_0\rangle = \sin[(2k+1)\theta] + \frac{1}{\sqrt{N-1}}\cos[(2k+1)\theta]\sum_{x\neq z}|x\rangle \tag{193}$$

が得られる. その結果 $U_f^k|\varphi_0\rangle$ を測定すると確率

$$P_{z,k} = \sin^2[(2k+1)\theta]. \tag{194}$$

で $|z\rangle$ が得られる.

この仕組みを以下の簡単な例で調べよう. まず $n = 4$ ととると $N = 2^4 = 16$ となる. 最初 $(k = 0)$ と U_f を k 回作用させた後の確率は

$$a_0^2 = b_0^2 = 1/16, \quad a_k^2 = \sin^2[(2k+1)\theta], \; b_k^2 = \frac{\cos^2[(2k+1)\theta]}{N-1},$$

で与えられる. ここに $\theta = \sin^{-1}(1/4)$ である. 図 16 ～ 19 は $z = 10$ にとったときの $k = 1, 2, 3, 4$ に対する確率分布を示している. 確率 a_k^2 は k に関して単調増加せずに，ある k で最大値 (今の

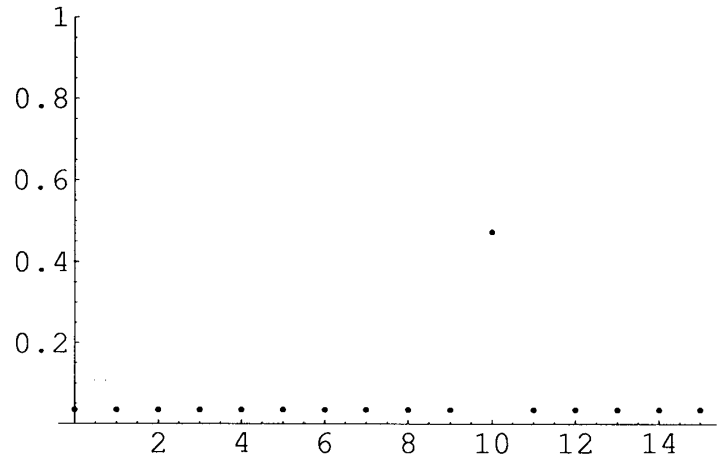


図 16: z を 10 にとったときの $U_f|\varphi_0\rangle$ の確率分布．横軸は z，縦軸は確率．

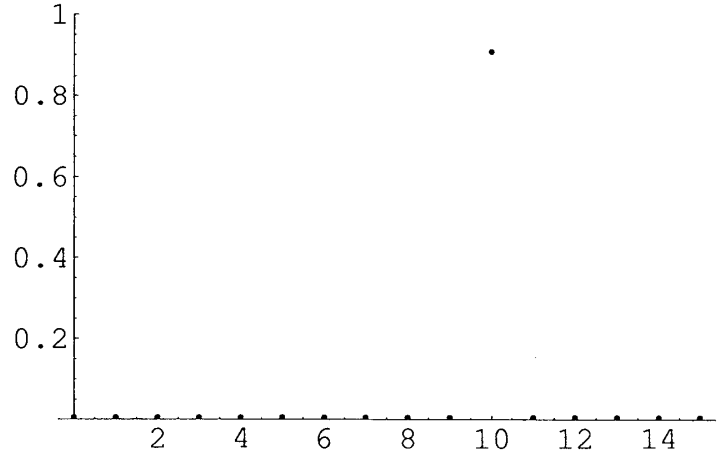


図 17: $k = 2$ にとったときの確率分布．

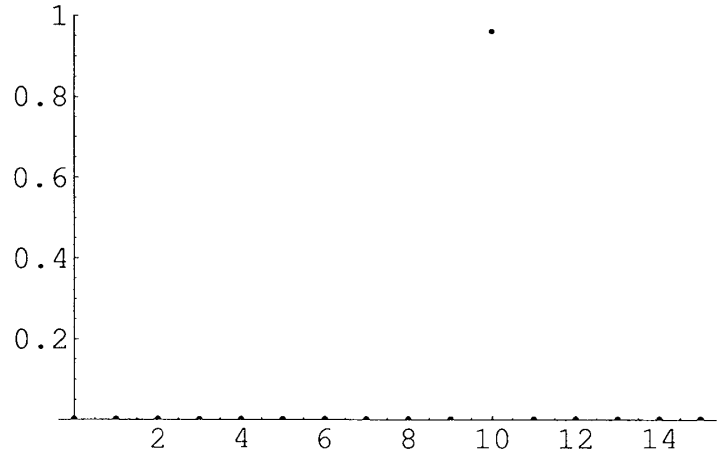


図 18: $k = 3$ にとったときの確率分布．

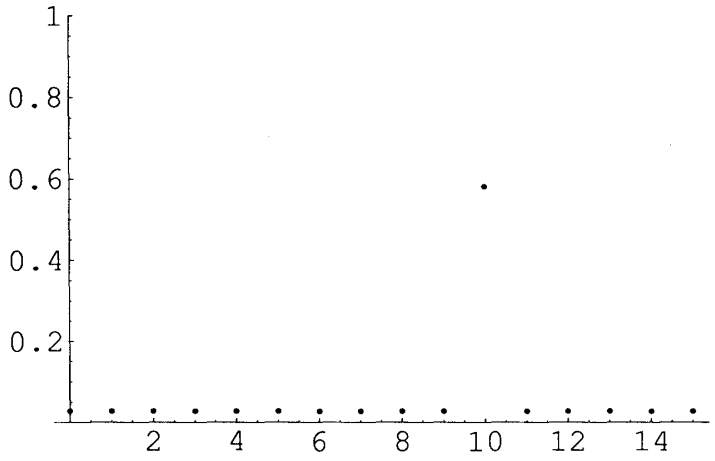


図 19: $k=4$ にとったときの確率分布.

場合は $k=3$) をとることに注意しよう.

STEP 4 最後に $P_{z,k}=a_k^2$ を最大にする k を求めよう. 大雑把に見積もるには

$$(2k+1)\theta=\frac{\pi}{2}\to k=\frac{1}{2}\left(\frac{\pi}{2\theta}-1\right) \tag{195}$$

と置けばよい. 上に述べた例では $k=3$ となっていたが, これは上の見積もり

$$\theta=\sin^{-1}(1/4)\simeq 0.25268\to k\simeq 2.6.$$

とよく合っている. この見積もりは次の命題により精密化される.

命題 7.4 $N=2^n\gg 1$ にたいし

$$m=\left[\frac{\pi}{4\theta}\right] \tag{196}$$

とする. ただし $[x]$ は Gauss の記号で, 実数 x を超えない最大の整数を表す. すると状態 $U_f^m|\varphi_0\rangle$ を観測すると, 我々が捜しているファイルが確率

$$P_{z,m}\geq 1-\frac{1}{N} \tag{197}$$

で得られる. また

$$m=O(\sqrt{N}) \tag{198}$$

である.

証明: 式 (196) から不等式 $\pi/4\theta-1<m\leq\pi/4\theta$ が得られる. $\tilde{m}$ を

$$(2\tilde{m}+1)\theta=\frac{\pi}{2}\to\tilde{m}=\frac{\pi}{4\theta}-\frac{1}{2}$$

で定義しよう. すると $|m-\tilde{m}|\leq 1/2$ から

$$|(2m+1)\theta-(2\tilde{m}+1)\theta|=\left|(2m+1)\theta-\frac{\pi}{2}\right|\leq\theta$$

となる．この不等式から

$$\cos^2[(2m+1)\theta] \leq \sin^2\theta = \frac{1}{N}$$

が得られる．したがって

$$P_{m,z} = \sin^2[(2m+1)\theta] = 1 - \cos^2[(2m+1)\theta] \geq 1 - \frac{1}{N}.$$

が示された．

また，$\theta > \sin\theta = 1/\sqrt{N}$ から

$$m = \left[\frac{\pi}{4\theta}\right] \leq \frac{\pi}{4\theta} \leq \frac{\pi}{4}\sqrt{N}$$

が示される．∎

この量子アルゴリズムは $O(\sqrt{N})$ のステップしか要しないことに注意されたい．それに対して古典的な検索アルゴリズムは $O(N)$ のステップを要する．

7.2　d 個のファイルの検索

ある与えられた条件を満たすファイルが d (>1) 個ある場合に，これらをすべて検索するアルゴリズムを考えよう．この問題はオラクル

$$f(x) = \begin{cases} 1 & (x \in A) \\ 0 & (x \notin A) \end{cases} \tag{199}$$

によって定式化される．ここに A は与えられた条件を満たす元すべてからなる S_n の部分集合である．もちろん我々は A を前もって知ってはいない．

この場合も単一ファイルの検索と同様に求めることができる．まず

$$R_f = I - 2\sum_{z\in A} |z\rangle\langle z| \tag{200}$$

を定義しよう．R_f を $|\varphi\rangle = \sum_{x=0}^{N-1} w_x|x\rangle$ (ただし $\sum_x |w_x|^2 = 1$) に作用させると

$$R_f|\varphi\rangle = \sum_{x\notin A} w_x|x\rangle - \sum_{z\in A} w_z|z\rangle \tag{201}$$

が得られる．

ここで

$$U_f = DR_f = (-I + 2|\varphi_0\rangle\langle\varphi_0|)\left(I - 2\sum_{z\in A}|z\rangle\langle z|\right) \tag{202}$$

を導入しよう．行列 $D = WRW$ は (180) で与えられている．U_f を $|\varphi\rangle$ に作用させると

$$U_f|\varphi\rangle = \sum_{x\notin A}(2\bar{w} - w_x)|x\rangle + \sum_{z\in A}(2\bar{w} + w_z)|z\rangle \tag{203}$$

となる．ただし

$$\bar{w} = \frac{1}{N}\left(\sum_{x\notin A} w_x - \sum_{z\in A} w_z\right) \tag{204}$$

である．

問 7.1 式 (203) を証明せよ．

問 7.2 $|\varphi_0\rangle = (1/\sqrt{N})\sum_{x=0}^{N-1}|x\rangle$ とするとき

$$U_f^k|\varphi_0\rangle = a_k \sum_{z\in A}|z\rangle + b_k \sum_{x\notin A}|x\rangle \tag{205}$$

を示せ．ただし $a_0 = b_0 = 1/\sqrt{N}$ および

$$a_k = \frac{N-d}{N}a_{k-1} + \frac{2(N-d)}{N}b_{k-1} \tag{206}$$

$$b_k = -\frac{2d}{N}a_{k-1} + \frac{N-2d}{N}b_{k-1} \tag{207}$$

である．ここに d は A の元の個数．

上の漸化式は簡単に解け

$$a_k = \frac{1}{\sqrt{d}}\sin[(2k+1)\theta], \quad b_k = \frac{1}{\sqrt{N-d}}\cos[(2k+1)\theta], \tag{208}$$

が得られる．ここに

$$\sin\theta = \sqrt{\frac{d}{N}}, \quad \cos\theta = \sqrt{1-\frac{d}{N}}. \tag{209}$$

問 7.3 式 (208) を証明せよ．

上の係数から $|\varphi_0\rangle$ に U_f を k 回作用させて得られる状態は

$$U_f^k|\varphi_0\rangle = \frac{1}{\sqrt{d}}\sin[(2k+1)\theta]\sum_{z\in A}|z\rangle + \frac{1}{\sqrt{N-d}}\cos[(2k+1)\theta]\sum_{x\notin A}|x\rangle \tag{210}$$

となることがわかる．

したがって状態を測定したときに，求めているファイル達が得られる確率を最大にするには

$$P_{A,k} = \sum_{z\in A}\left(\frac{1}{\sqrt{d}}\sin[(2k+1)\theta]\right)^2 = \sin^2[(2k+1)\theta] \tag{211}$$

を最大にすればよい．単一ファイル検索のときの議論を繰り返すことにより，$d \ll N$ のときは以下の結果が得られる．整数

$$m = \left[\frac{\pi}{4\theta}\right] \tag{212}$$

にたいし，状態 $U_f^m|\varphi_0\rangle$ を観測したとき A の中のファイルの一つが得られる確率は

$$P_{A,m} \geq 1 - \frac{d}{N} \tag{213}$$

で与えられる．さらに

$$m = O(\sqrt{N/d}) \tag{214}$$

である．

問 7.4 式 (213) と (214) を証明せよ．

8 Shor's Factorisation Algorithm

Shor の素因数分解アルゴリズムは量子コンピュータが古典コンピュータに比べ「指数関数的に」強力である一例である [12]．素因数分解を古典コンピュータで実行すると量子版に比べ入力ビット数の指数関数的に多くの時間がかかり，事実上実行不可能となる．実際，Shor のアルゴリズムはほとんど古典版と同じであるが，一点だけが量子コンピュータで置き換えられている．まず，大きな数の素因数分解がなぜ重要か調べよう．

8.1 RSA 暗号システム：素因数分解がなぜ重要か？

RSA 公開鍵暗号システムはインターネットなどでメッセージを暗号化して伝えるのに日常使われている．これは大前提「大きな数を素因数に分解するには途方もない時間がかかる」に基づいている．

RSA 暗号 [11] はこの事実をもちいてメッセージをエンコード，デコードする．以下の例を考えよう．Alice が Bob にメッセージを送る：

1. Alice は大きな素数 p と q を選びそれを秘密にしておく．彼女はその積 $N = pq$ を求め，それを公開する．たとえば

$$p = 928101320540413151847590244727697333896 9,$$

$$q = 959171534923719499954705006871893051427 9,$$

にたいして

$$\begin{aligned} N \;=\; & 890208368187479079568319892720916003036132646037942 47 \\ & 032637647625631554961638351, \end{aligned}$$

n の桁数が多いとこれを p, q に素因数分解するには膨大な時間がかかる．Alice はまた指数 e $(< N)$ と呼ばれる整数を用意する．e は $(p-1)(q-1)$ と素でなければならない．これは簡単に求められ，たとえば

$$e = 1234567,\ \gcd(e, (p-1)(q-1)) = 1.$$

e も n と同様に公開されている．

2. Bob は Alice に "hallo" というメッセージを送りたい．彼はこれを n より小さな 10 進数の列として送る．彼のスキームで，そのメッセージが

$$\text{hello} = 12300045600078900123,$$

となったとしよう．彼はこれを $\text{hello}^e \pmod N$ としてエンコードし，それを公開されたチャネルで Alice に送信する：

$$\begin{aligned}\text{encrypted} \equiv \text{hello}^e \pmod N = {} & 37853991457169688722835964472412 \\ & 30264989670986991169935543701913266864573727079 9\end{aligned}$$

3. Alice は受け取ったメッセージをデコードする．まず彼女は e の modulo $(p-1)(q-1)$ に関する逆 d を求める:

$$\begin{aligned} de &\equiv 1 \pmod{(p-1)(q-1)} \rightarrow \\ d &= 37853991457169688722835964472412302649896709869911699355437019132668645737270799 \end{aligned}$$

次に彼女は暗号化されたメッセージをデコードする：

$$\text{encrypted}^d \pmod N \equiv 12300045600078900123 = \text{hello}.$$

このシステムは「大きな数の素因数分解にとてつもない時間がかかる」すなわち「N, e が公開されているにもかかわらず，この世で p, q を知っているのは Alice だけである」という神話に基づいている．Shor のアルゴリズムはこの神話を打ち砕いた．

8.2 素因数分解アルゴリズム

p と q を素数とし $N = pq$ とする．N を p と q に素因数分解したい．ナイーヴには p と q を見つけるまでに最悪 $\sqrt{N}$ 回の試行錯誤が必要となる．$N \sim 2^n$ にたいし $\sqrt{N} = e^{(n/2)\ln 2}$ であるからこの方法は効率的ではない．この問題に量子アルゴリズムを適用するには以下のスキームが適している．

STEP 1: N より小さな正の整数 m をランダムに選び Euclid の互除法で $\gcd(m, N)$ を求める．それが 1 でなければ，m は p か q であり問題は解けた．そこで $\gcd(m, N) = 1$ であるとしよう．

STEP 2: $f_N : \mathbb{N} \to \mathbb{N}$ を $a \mapsto m^a \pmod N$ で定義する．$m^P \equiv 1 \pmod N$ を満たす最小の $P \in \mathbb{N}$ を求める．この数 P を**周期 (period)** という．(古典的に P を求めるには $\log_2 N$ の指数関数だけのステップが必要であることが知られている．量子アルゴリズムではこれが多項式ステップですむ．量子コンピュータが必要とされるのはこのステップだけである．後のステップは古典

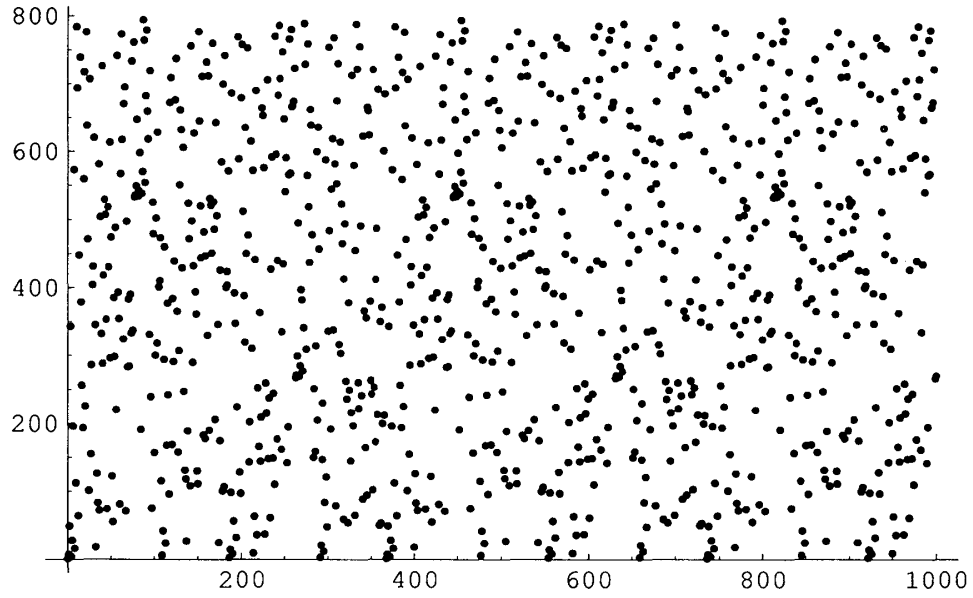


図 20: $7^x \pmod{799}$ のグラフ．横軸は x.

アルゴリズムで十分効率的に計算できる．)

STEP 3: P が奇数であれば以下で用いることができないのでSTEP 1に戻り別の m を採用する．P は偶数として次に進む．

STEP 4: P は偶数であるから

$$(m^{P/2}-1)(m^{P/2}+1) = m^P - 1 \equiv 0 \pmod{N}. \tag{215}$$

が成り立つ．もし $m^{P/2}+1 \equiv 0 \pmod{N}$ であれば $\gcd(m^{P/2}-1, N) = 1$ であり，STEP 1に戻り別の m でやり直す．もし $m^{P/2}+1 \not\equiv 0 \pmod{N}$ であれば $m^{P/2}-1$ は p か q を含んでおりSTEP 5へ進む．($m^{P/2}-1$ は N の倍数ではありえない．もしそうであれば $m^{P/2} \equiv 1 \pmod{N}$ となってしまうが，これは P が $m^P \equiv 1 \pmod{N}$ を満たす最小の数であるという定義に矛盾.)

STEP 5:

$$d = \gcd(m^{P/2}-1, N) \tag{216}$$

は p または q となり，素因数分解が完了する．

例 8.1 $N = 799 = 17 \cdot 47$ としよう．もちろん素因数17と47は知らないふりをする．

STEP 1: $m = 7$ ととると $\gcd(799, 7) = 1$ でOK.

STEP 2: 図20から $7^{368} \equiv 1 \pmod{799}$ であるので $P = 368$.

STEP 3: P は偶数 $(P/2 = 184)$ なので STEP 4 へ進む.

STEP 4: $(7^{184} - 1)(7^{184} + 1) \equiv 0 \pmod{799}$. すぐわかるように $\gcd(7^{184} + 1, 799) = 17 \neq 1$ であるから STEP 5 へ.

STEP 5: $7^{184} - 1$ と $N = 799$ は共通の素数因子を持っている. 実際 $d = \gcd(7^{184} - 1, 799) = 47$. $799/47 = 17$ から $799 = 47 \cdot 17$ が得られる.

量子計算が必要なのは P を求める STEP 2 だけである. 以下に示すように量子計算で得られる'周期' P' は P そのものとは限らず, P の整数倍のときもある. もし $P' = 2kP$ $(k \in \mathbb{N})$ であれば, 素因数は $m^{P'/2} - 1$ からは求められない. なぜならば

$$m^{P'/2} - 1 = m^{kP} - 1 = (aN + 1)^k - 1 = AN \equiv 0 \pmod{N}$$

となるからである. A はある整数. ここに $m^P = aN + 1$ を用いた. 一方 $P' = (2k + 1)P$ であれば

$$m^{P'/2} - 1 = m^{kP} m^{P/2} - 1 = (aN + 1)^k m^{P/2} - 1 \equiv m^{P/2} - 1 \pmod{N}$$

となって $\gcd(m^{P'/2} - 1, N)$ は自明でない素因数を生成する.

問 8.1 $N = 35$ とせよ. 上のステップを繰り返し N の素因数を求めよ. (その周期 P が 10 よりも小さな m が存在する. もし不運にも $P > 10$ となりそうであれば別の m を捜したほうがよい. 幸運を祈る.)

8.3 STEP 2 の詳細

$N = pq \in \mathbb{N}$ を素因数分解するべき数とし,

$$N^2 \leq 2^n < 2N^2 \tag{217}$$

を満たす $n \in \mathbb{N}$ を見つけよ. 関数 $f : a \mapsto m^a \pmod{N}$ を

$$S_n = \{0, 1, \ldots, 2^n - 1\} \tag{218}$$

の上に制限したものを同じ記号 $f : S_n \to S_n$ で定義する[10].

量子コンピュータには 2 組の n 量子ビットレジスターがあるとし, それを $|\mathrm{REG1}\rangle$ と $|\mathrm{REG2}\rangle$ とする:

$$|\mathrm{REG1}\rangle|\mathrm{REG2}\rangle = |a\rangle|b\rangle = |a_{n-1} \ldots a_1 a_0\rangle|b_{n-1} \ldots b_1 b_0\rangle \tag{219}$$

ただし

$$a = \sum_{j=0}^{n-1} a_j 2^j, \; b = \sum_{j=0}^{n-1} b_j 2^j.$$

[10] $0 \leq f(S_n) \leq N - 1 \leq \sqrt{2^n} - 1 < 2^n - 1$ より f の値域が S_n であることは明らかである.

レジスターの中の数は $0 \leq a, b \leq 2^n - 1$ を満たす.

以下では n 量子ビット系の離散 Fourier 変換 (DFT)

$$|x\rangle \to \mathcal{F}|x\rangle \equiv \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega^{-xy}|y\rangle \tag{220}$$

を用いる. ここに $x, y \in S_n$ で $\omega = \exp(2\pi i/2^n)$ である. 以下 DFT を $\mathcal{F}$ で表す.

STEP 2 を更に詳しく調べよう :

STEP 2.0: 2つのレジスターを初期状態

$$|\psi_0\rangle = |\mathrm{REG1}\rangle|\mathrm{REG2}\rangle = |0\rangle|0\rangle = |\underbrace{00\ldots0}_{n\text{ 量子ビット}}\rangle|\underbrace{00\ldots0}_{n\text{ 量子ビット}}\rangle \tag{221}$$

に設定する.

STEP 2.1: $|\mathrm{REG1}\rangle$ に $\mathcal{F}$ を作用させる :

$$|\psi_0\rangle = |0\rangle|0\rangle \overset{\mathcal{F}\otimes I}{\mapsto} |\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \omega^{-0\cdot x}|x\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle. \tag{222}$$

したがって REG1 は $|x\rangle$ $(0 \leq x \leq 2^n - 1)$ のすべての状態の重ねあわせになっている.

STEP 2.2: $m < N$, $gcd(m, N) = 1$ を満たす m をとり, 関数 $f : S_n \to S_n$ を

$$f(x) = m^x \pmod N, \quad x \in S_n. \tag{223}$$

で定義する. ユニタリーゲート U_f は関数 f の x にたいする作用を $U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$ のように実現するとしよう. STEP 2.1 で得られた状態に U_f を作用させる :

$$U_f|\psi_1\rangle = |\psi_2\rangle \equiv \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle. \tag{224}$$

その結果2つのレジスターは entangle する.

STEP 2.3: DFT を $|\mathrm{REG1}\rangle$ に作用させる

$$\begin{aligned} |\psi_3\rangle &= (\mathcal{F}\otimes I)|\psi_2\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} \omega^{-xy}|y\rangle|f(x)\rangle \\ &= \frac{1}{2^n} \sum_{y=0}^{2^n-1} |y\rangle|\Upsilon(y)\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \||\Upsilon(y)\rangle\| \cdot |y\rangle \frac{|\Upsilon(y)\rangle}{\||\Upsilon(y)\rangle\|} \end{aligned} \tag{225}$$

ただし

$$|\Upsilon(y)\rangle = \sum_{x=0}^{2^n-1} \omega^{-xy}|f(x)\rangle. \tag{226}$$

STEP 2.4: $|\mathrm{REG1}\rangle$ を測定する．その結果 $y_0 \in S_n$ を観測する確率は

$$\mathrm{Prob}(y_0) = \frac{\||\Upsilon(y_0)\rangle\|^2}{2^{2n}} \tag{227}$$

である．同時に状態は

$$|y_0\rangle \frac{|\Upsilon(y_0)\rangle}{\||\Upsilon(y_0)\rangle\|}$$

へと収縮する．

観測値 $y \in S_n$ が得られる確率は確率分布

$$\mathrm{Prob}(y) = \frac{\||\Upsilon(y)\rangle\|^2}{2^{2n}}$$

に従う．

STEP 2.5: 周期 P を観測値の確率分布から読み取る．

8.4 確率分布

確率分布 $\mathrm{Prob}(y)$ を詳細に調べよう．

命題 8.1 $Q \equiv 2^n = Pq + r$, $(0 \le r < P)$ とする．ただし q と r は一意的に決まる非負の整数．$Q_0 = Pq$ とする．このとき

$$\mathrm{Prob}(y) = \begin{cases} \dfrac{r\sin^2\left(\frac{\pi Py}{Q}\left(\frac{Q_0}{P}+1\right)\right) + (P-r)\sin^2\left(\frac{\pi Py}{Q}\cdot\frac{Q_0}{P}\right)}{Q^2\sin^2\left(\frac{\pi Py}{Q}\right)} & (Py \not\equiv 0 \pmod{Q}) \\ \dfrac{r(Q_0+P)^2 + (P-r)Q_0^2}{Q^2P^2} & (Py \equiv 0 \pmod{Q}) \end{cases} \tag{228}$$

証明: 定義から

$$\begin{aligned} |\Upsilon(y)\rangle &= \sum_{x=0}^{Q-1} \omega^{-xy}|f(x)\rangle \\ &= \sum_{x=0}^{Q_0-1} \omega^{-xy}|f(x)\rangle + \sum_{x=Q_0}^{Q-1} \omega^{-xy}|f(x)\rangle \\ &= \sum_{x_0=0}^{P-1}\sum_{x_1=0}^{Q_0/P-1} \omega^{-(Px_1+x_0)y}|f(Px_1+x_0)\rangle + \sum_{x_0=0}^{r-1} \omega^{-[P(Q_0/P)+x_0]y}|f(P(Q_0/P)+x_0)\rangle \\ &= \sum_{x_0=0}^{P-1} \omega^{-x_0y}\left(\sum_{x_1=0}^{Q_0/P-1}\omega^{-Px_1y}\right)|f(x_0)\rangle + \sum_{x_0=0}^{r-1}\omega^{-x_0y}\omega^{-Py(Q_0/P)}|f(x_0)\rangle \\ &= \left(\sum_{x_0=0}^{r-1}+\sum_{x_0=r}^{P-1}\right)\omega^{-x_0y}\sum_{x_1=0}^{Q_0/P-1}\omega^{-Pyx_1}|f(x_0)\rangle + \sum_{x_0=0}^{r-1}\omega^{-x_0y}\omega^{-Py(Q_0/P)}|f(x_0)\rangle \end{aligned}$$

$$= \sum_{x_0=0}^{r-1} \omega^{-x_0 y} \left(\sum_{x_1=0}^{Q_0/P} \omega^{-Pyx_1} \right) |f(x_0)\rangle + \sum_{x_0=r}^{P-1} \omega^{-x_0 y} \left(\sum_{x_1=0}^{Q_0/P-1} \omega^{-Pyx_1} \right) |f(x_0)\rangle.$$

写像 $f : a \mapsto m^a \pmod N$ は $\{0,1,2,\ldots,P-1\}$ 上 1 : 1 である．[11] したがって $|f(0)\rangle, |f(1)\rangle, \ldots, |f(P-1)\rangle$ は互いに直交している．したがって

$$\langle \Upsilon(y)|\Upsilon(y)\rangle = r \left| \sum_{x_1=0}^{Q_0/P} \omega^{-Pyx_1} \right|^2 + (P-r) \left| \sum_{x_1=0}^{Q_0/P-1} \omega^{-Pyx_1} \right|^2.$$

$Py \equiv 0 \pmod Q$ の場合は

$$\omega^{-Pyx_1} = e^{-2\pi i(Py/Q)x_1} = e^{-2\pi i n x_1} = 1, \quad (Py = nQ).$$

したがって

$$\langle \Upsilon(y)|\Upsilon(y)\rangle = r \left(\frac{Q_0}{P} + 1 \right)^2 + (P-r) \left(\frac{Q_0}{P} \right)^2,$$

となり y によらない結果を得る：

$$\mathrm{Prob}(y) = \frac{r(Q_0+P)^2 + (P-r)Q_0^2}{P^2Q^2} = \frac{r(q+1)^2 + (P-r)q^2}{Q^2}. \tag{229}$$

$Py \not\equiv 0 \pmod Q$ のときは

$$\begin{aligned} \langle \Upsilon(y)|\Upsilon(y)\rangle &= r \left| \frac{\omega^{-Py(Q_0/P+1)} - 1}{\omega^{-Py} - 1} \right|^2 + (P-r) \left| \frac{\omega^{-Py(Q_0/P)} - 1}{\omega^{-Py} - 1} \right|^2 \\ &= r \left| \frac{e^{-(2\pi i/Q)Py(Q_0/P+1)} - 1}{e^{-(2\pi i/Q)Py} - 1} \right|^2 + (P-r) \left| \frac{e^{-(2\pi i/Q)Py(Q/P)} - 1}{e^{-(2\pi i/Q)Py} - 1} \right|^2. \end{aligned}$$

したがって

$$|e^{i\theta} - 1|^2 = (\cos\theta - 1)^2 + \sin^2\theta = 2(1 - \cos\theta) = 4\sin^2\frac{\theta}{2}$$

から

$$\langle \Upsilon(y)|\Upsilon(y)\rangle = r \frac{\sin^2 \frac{\pi}{Q} Py \left(\frac{Q_0}{P} + 1 \right)}{\sin^2 \frac{\pi}{Q} Py} + (P-r) \frac{\sin^2 \frac{\pi}{Q} Py \frac{Q_0}{P}}{\sin^2 \frac{\pi}{Q} Py}$$

となる．よって確率分布は

$$\mathrm{Prob}(y) = \frac{\| |\Upsilon(y)\rangle \|^2}{Q^2} = \frac{r \sin^2 \left[\frac{\pi}{Q} Py \left(\frac{Q_0}{P} + 1 \right) \right] + (P-r) \sin^2 \left[\frac{\pi}{Q} Py \frac{Q_0}{P} \right]}{Q^2 \sin^2 \frac{\pi}{Q} Py} \tag{230}$$

となり命題が証明された．∎

[11] もし $m^a \equiv m^b \pmod N$ $(0 \le b < a \le P-1)$ であれば $m^b(m^{a-b} - 1) \equiv 0 \pmod N$ である．m と N は互いに素であるので m^b と N も互いに素である．すると $m^P > m^{a-b} \equiv 1 \pmod N$ となるが，これは矛盾．

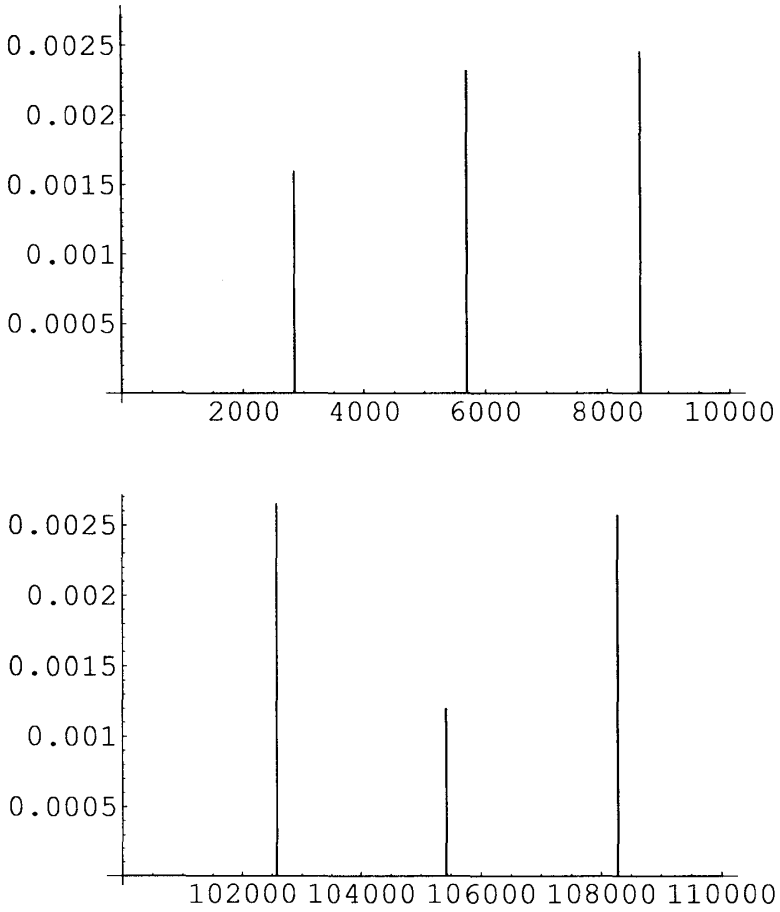


図 21: (a) $N = 799, m = 7, P = 368$ のときの領域 $0 \leq y \leq 10,000$ における確率分布 $\mathrm{Prob}(y)$. (b) 領域 $100,000 \leq y \leq 110,000$ における確率分布.

系 8.1 $Q/P \in \mathbb{N}$ とする (すなわち $Q_0 = Q$). すると確率分布は

$$\mathrm{Prob}(y) = \begin{cases} 0 & (Py \not\equiv 0 \pmod{Q}) \\ \dfrac{1}{P} & (Py \equiv 0 \pmod{Q}) \end{cases} \tag{231}$$

証明: $Py \not\equiv 0 \pmod{Q}$ のとき $r = 0$ であるから $Q = Pq$. したがって

$$\mathrm{Prob}(y) = \frac{P \sin^2 \pi y}{Q^2 \sin^2 \frac{\pi y}{q}} = 0.$$

$Py \equiv 0 \pmod{Q}$ のときは

$$\mathrm{Prob}(y) = \frac{PQ^2}{Q^2 P^2} = \frac{1}{P}.$$

∎

図 21 は $\mathrm{Prob}(y)$ を $N = 799 = 17 \cdot 47, P = 368, Q = 2^{20} = 1,048,576$ のときに示したものである. $N^2 = 638,401$ および $2N^2 = 1,276.802$ より $N^2 < Q < 2N^2$ となることに注意せよ. す

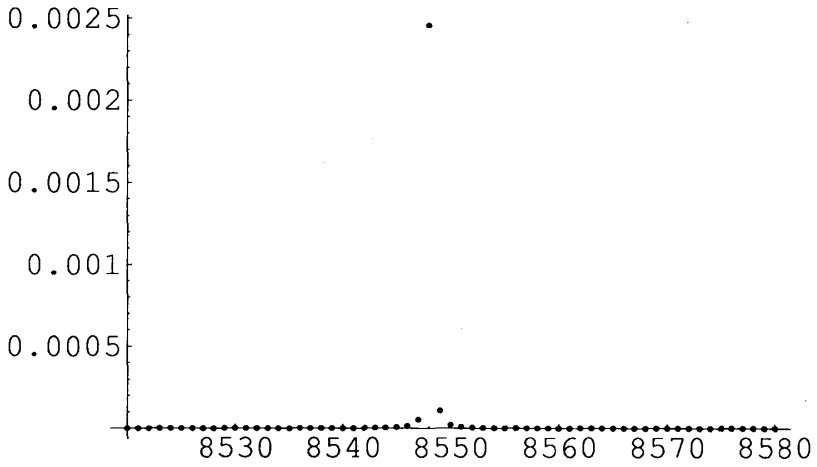


図 22: 領域 $8,520 \leq y \leq 8,580$ における確率分布 $\mathrm{Prob}(y)$. 条件は前の図と同じ.

ると $Q \equiv 144 \pmod{368} \to r = 144, Q_0 = Q - r = 1,048,432, \to q = Q_0/P = 2,849$ となる. したがって $\mathrm{Prob}(y)$ は $q = 2,849$ の整数倍のところに鋭いピークを持つ. 図 22 は $\mathrm{Prob}(y)$ を $8,520 < y < 8,580$ でプロットしたものである. $y = 8548$ に鋭いピークが見られる. このとき $8548/2849 = 3.00035$. 以下の確率を比較せよ :

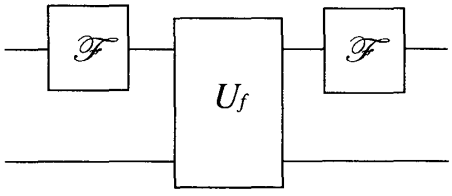
$$\mathrm{Prob}(8547) = 0.00005393,\ \mathrm{Prob}(8548) = 0.00245753,\ \mathrm{Prob}(8549) = 0.00010892.$$

その近傍の数にたいしては $8547/2849 = 3, 8549/2849 = 3.0007$ である. 全領域を見渡すと $P = 368$ 個の鋭いピークが存在し, 各ピークにおいて $\mathrm{Prob}(y)$ はほぼ $1/386 \sim 0.00272$ となる.

y は $0 \leq y \leq Q - 1$ に制限されているので, 測定を繰り返すことによりピークの間隔が 2849 であることが分かる. これは周期の近似値 $P = Q/2849 \sim 368.0505$ を与える. これが正しいかどうかは STEP 3 ~ STEP 5 を実行しなければならない. (ピークの間隔が 2850 と見積もられても $P \sim Q/2850 \simeq 367.9212$ から $P = 368$ が推測される. §8.2 に示したように $P = 368$ は正しい素因数 17 と 47 をあたえる.

8.5　まとめ

量子アルゴリズムを用いて $N = pq$ の素因数分解が効率よく実行できることを示した. 量子アルゴリズムは関数 $f(x) = m^x \pmod{N}$ の周期を求めるためにのみ使われ, それ以外は古典コンピュータで実行できる. 量子アルゴリズムは次の量子回路で構成される :



ここに U_f は写像 $U_f|x\rangle|0\rangle = |x\rangle|m^x \pmod N\rangle$ を，$\mathcal{F}$ は DFT を表す．

STEP 2 を再び前出の例を用いてまとめよう．

STEP 2.0: 初期状態

$$|\psi_0\rangle = |0\rangle|0\rangle. \tag{232}$$

STEP 2.1: 第 1 レジスターに DFT を作用させる：

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|0\rangle, \tag{233}$$

ここに $Q = 2^{20} = 1048576$.

STEP 2.2: U_f を作用させ状態

$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|7^x \pmod{799}\rangle \\
&= \frac{1}{\sqrt{Q}}\Big[|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|49\rangle + |3\rangle|343\rangle + |4\rangle|4\rangle + |5\rangle|28\rangle \\
&\quad +\ldots \\
&\quad +|Q-2\rangle|756\rangle + |Q-1\rangle|498\rangle\Big]
\end{aligned} \tag{234}$$

を生成する．第 2 レジスターは周期 $P = 368$ で周期的であることに注意．

STEP 2.3: $\omega = e^{2\pi i/Q}$ の DFT を第 1 レジスターに作用させる．その結果は

$$\begin{aligned}
|\psi_3\rangle &= \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}\frac{1}{\sqrt{Q}}\sum_{y=0}^{Q-1}\omega^{-xy}|y\rangle|7^x \pmod{799}\rangle \\
&= \frac{1}{Q}\sum_{y=0}^{Q-1}\sum_{x=0}^{Q-1}\omega^{-xy}|7^x \pmod{799}\rangle \\
&\equiv \frac{1}{Q}\sum_{y=0}^{Q-1}|y\rangle|\Upsilon(y)\rangle,
\end{aligned} \tag{235}$$

ただし

$$\begin{aligned}
|\Upsilon(y)\rangle &= \sum_{x=0}^{Q-1}\omega^{-xy}|7^x \pmod{799}\rangle \\
&= |1\rangle + \omega^{-y}|7\rangle + \omega^{-2y}|49\rangle + \omega^{-3y}|343\rangle + \ldots \\
&\quad +\omega^{-368y}|1\rangle + \omega^{-369y}|7\rangle + \omega^{-370y}|49\rangle + \omega^{-371y}|343\rangle + \ldots \\
&\quad +\ldots + \\
&\quad +\omega^{-736y}|1\rangle + \omega^{-737y}|7\rangle + \omega^{-738y}|49\rangle + \omega^{-739y}|343\rangle + \ldots \\
&\quad +\ldots + \\
&\quad +\omega^{-1048432y}|1\rangle + \omega^{-1048433y}|7\rangle + \omega^{-1048434y}|49\rangle + \omega^{-1048435y}|343\rangle \\
&\quad \ldots + \omega^{-1048575y}|498\rangle
\end{aligned}$$

$$
\begin{aligned}
= \; & (1+\omega^{-368y}+\omega^{-736y}+\ldots+\omega^{-1048432y})|1\rangle \\
& +(\omega^{y}+\omega^{-369y}+\omega^{-737y}+\ldots+\omega^{-1048433y})|7\rangle \\
& +(\omega^{-2y}+\omega^{-370y}+\omega^{-738y}+\ldots+\omega^{-1048434y})|49\rangle \\
& +(\omega^{-3y}+\omega^{-371y}+\omega^{-739y}+\ldots+\omega^{-1048435y})|-343\rangle \\
& \qquad\qquad +\ldots \\
& +(\omega^{-87y}+\omega^{-455y}+\omega^{-823}+\ldots)|794\rangle. \qquad (236)
\end{aligned}
$$

この展開には368のケットベクトルが存在する．各ベクトルの係数はyが2849の整数倍に近いときにのみ大きくなる．例えば

$$
\sum_{x=0}^{2849}\omega^{-368ky}=0.608696+0.000262611i, \quad (y=1)
$$

であるが

$$
\begin{aligned}
\sum_{x=0}^{2849}\omega^{-368ky} &= 731.803+2058i, \quad (y=2849) \\
&= 2315.79+1408.03I, \quad (y=8548).
\end{aligned}
$$

となる．このように前節の結果

$$
\mathrm{Prob}(8548)=368\left(\frac{|2315.79+1408.03i|}{Q}\right)^{2}=0.00245848 \qquad (237)
$$

が再現される．

9　NMR量子コンピュータ

量子コンピュータを実現するには，それを実装する物理系が必要である．現在までに(1) トラップされたイオン (2) 中性原子 (3) 室温および低温NMR (4) 超伝導Josephson接合 (5) 量子ドット (6) キャビティQED(7) 光学的アプローチ (8) ヘリウム液面上の電子系など様々な系がその候補として研究されている．現在最大の量子コンピュータは7量子ビットの分子を用いたNMR量子コンピュータである．室温で液体に溶かした分子を使うNMRでは分子は熱分布をしており，以下に見るように初期状態として基底状態の寄与のみを取り出すには工夫と手間が要る．また，本当にもつれた状態が実現しているのか疑問もある．そのため液体NMRが本当に量子コンピュータかどうかは議論が分かれるが，これまで述べた量子アルゴリズムを実装するには恰好の手段である．以下ではNMR量子コンピュータの概略を解説した後，講義では触れられなかった我々の最近の結果を紹介する．

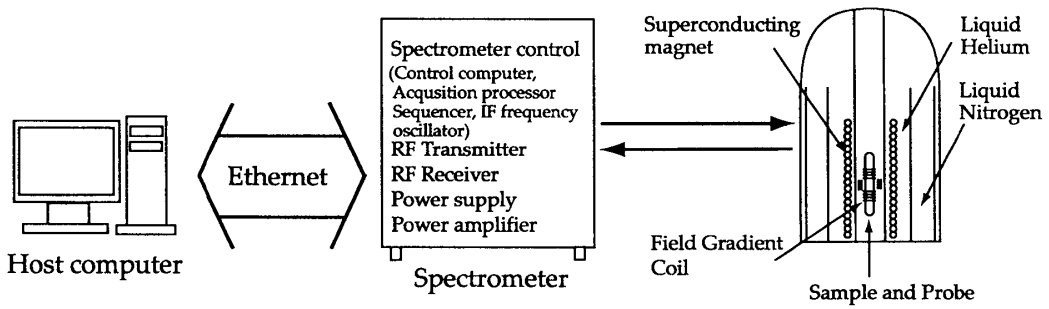


図 23: 標準的な NMR 装置の概略．左のサンプルには超伝導磁石で生成された z 軸向きの強力な磁場がかかっており，それに垂直な xy 面方向の振動磁場により分子のスピン状態を制御する．液体窒素と液体ヘリウムは超伝導磁石を冷却するもので，サンプルは室温程度の温度に保たれる．中央のスペクトロメータは振動磁場を発生し，またデータ取得パルスをかけた後，サンプル中の分子が発生する誘導起電力を受信してそれをフーリエ変換し，必要なスペクトルを得る．右側のコンピュータには振動磁場の振幅や位相を楽譜のように入力し，指定された振幅や位相を持つパルスが決められたタイミングでサンプルに供給されるようスペクトロメータの発振機を制御する．

9.1 NMR 量子コンピュータ

9.1.1 1 量子ビット ハミルトニアン

NMR 装置（図 23）の中で，分子には超伝導磁石で生成した $\sim$ 10T 程度の強力な磁束密度 $\boldsymbol{B}_0$ が z 方向に加えられている．それにより分子中のスピン 1/2 の核はスピン上向きと下向きでエネルギー差 $\hbar\omega_0$ をもつ．ただし $\omega_0 = \hbar\gamma B_0$ は Larmor 振動数．今分子の中にはスピン 1/2 をもつ核が 1 個あるとしよう．するとハミルトニアンは

$$H_0 = -\hbar\omega B_0 \frac{\sigma_z}{2} \tag{238}$$

で与えられる．ただし上向きスピンを $|0\rangle = (1,0)^T$，下向きスピンを $|1\rangle = (0,1)^T$ で表す．

さらに NMR 装置には $\boldsymbol{B}_0$ に垂直に振動磁場

$$\boldsymbol{B}_1(t) = B_1 \cos(\omega_{\rm rf} t)(\cos\varphi, \sin\varphi, 0)^T \tag{239}$$

を発生する送信機とコイルが備わっている．B_1 は磁場の振幅，$\omega_{\rm rf}$ はその振動数，φ は xy 面内の位相角である．ここで $\boldsymbol{B}_1$ を時計回りと反時計回りの成分に分離する:

$$\boldsymbol{B}_1(t) = \frac{B_1(t)}{2}\left(\cos(\omega_{\rm rf}t+\varphi) + \cos(-\omega_{\rm rf}t+\varphi), \sin(\omega_{\rm rf}t+\varphi) + \sin(-\omega_{\rm rf}t+\varphi), 0\right)^T. \tag{240}$$

すると，このスピンのハミルトニアンは

$$\begin{aligned} H &= -\gamma\hbar B_1 \left[\{\cos(\omega_{\rm rf}t+\varphi) + \cos(-\omega_{\rm rf}t+\varphi)\}\frac{\sigma_x}{2} + \{\sin(\omega_{\rm rf}t+\varphi)) + \sin(-\omega_{\rm rf}t+\varphi)\}\frac{\sigma_y}{2}\right] \\ &\quad -\hbar\omega_0\frac{\sigma_z}{2} \end{aligned} \tag{241}$$

となる．

このハミルトニアンは核が $\omega_{\rm rf}$ で回転している系にゲージ変換すると簡単になる．そのために

$$|\psi\rangle_{\rm rot} \equiv \exp\left(i\omega_{\rm rf}\sigma_z t/2\right)|\psi\rangle \tag{242}$$

とおく．すると $|\psi\rangle_{\rm rot}$ が満たすシュレーディンガー方程式は

$$\begin{aligned} i\frac{\partial}{\partial t}|\psi\rangle_{\rm rot} &= \left[-\hbar\Delta\omega\frac{\sigma_z}{2} - \frac{\gamma\hbar B_1}{2}\begin{pmatrix} 0 & e^{-i\varphi}(1+e^{2i\omega_{\rm rf}t}) \\ e^{i\varphi}(1+e^{-2i\omega_{\rm rf}t}) & 0 \end{pmatrix}\right]|\psi\rangle_{\rm rot} \\ &\simeq \left[-\hbar\Delta\omega\frac{\sigma_z}{2} - \gamma\hbar B_1\left(\cos\varphi\frac{\sigma_x}{2} + \sin\varphi\frac{\sigma_y}{2}\right)\right]|\psi\rangle_{\rm rot} \equiv H_{\rm rot}|\psi\rangle_{\rm rot} \end{aligned} \tag{243}$$

となる．ここで $\Delta\omega = \omega_0 - \omega_{\rm rf}$ で，2行目では周波数 $2\omega_{\rm rf}$ で振動する項を無視した．これは「**回転波近似**」とよばれ，この章では常にこの近似を用いる．以下，常にこの変換された系で話をし，記号を簡単にするために添え字 rot を落とす．また，実際の実験では共鳴条件 $\omega_0 = \omega_{\rm rf}$，すなわち $\Delta\omega = 0$ にとることが多く (例 3.2)，ここでもそのようにおく．結局1スピンのハミルトニアンは

$$H = -\hbar\omega_1\left(\cos\varphi\frac{\sigma_x}{2} + \sin\varphi\frac{\sigma_y}{2}\right) \tag{244}$$

と書かれた．ここで $\omega_1 = \gamma B_1$.

この (244) は ω_1, φ が定数である限り時間に依存せず扱い易い．我々は $-\hbar\omega_0\sigma_z/2$ を落とし，本質的に相互作用表示に移ったことに注意されたい．実際の実験では ω_1, φ は区分的に一定にとることが多い．このような場合は時間推進の演算子は

$$U = \mathcal{T}e^{-i\int_0^T H(t)dt} \equiv e^{-iH(t_n)\Delta t_n/\hbar}e^{-iH(t_{n-1})\Delta t_{n-1}/\hbar}\cdots e^{-iH(t_1)\Delta t_1/\hbar}, \tag{245}$$

で与えられる．ここに $\mathcal{T}$ は時間順序積で

$$H(t_k) = -\hbar\omega_1(t_k)\left(\cos\varphi(t_k)\frac{\sigma_x}{2} + \sin\varphi(t_k)\frac{\sigma_y}{2}\right)$$

は k 番目のステップのハミルトニアンである．

ここで一つ注意をする．ハミルトニアン (244) は $\mathrm{tr}H = 0$ を満たすので $U \in \mathrm{SU}(2)$ となる．実際

$$\det e^{-iHt/\hbar} = e^{\mathrm{tr}\,(-iHt/\hbar)} = 1.$$

量子力学では全体の位相は意味を持たないので，これは特に制限を与えない．どんな $U \in \mathrm{U}(2)$ に対しても $\tilde{U} = e^{i\alpha}U \in \mathrm{SU}(2)$ となるような位相 $e^{i\alpha}$ が存在するのである．

9.1.2　多量子ビット ハミルトニアン

スピン 1/2 をもつ核が2個ある分子を考える．ただし核の種類は異なり，そのためにそれぞれの Larmor 振動数 ω_{10} と ω_{20} は典型的に数百 MHz 異なるものとする．2個核があると，核のスピン間にハイゼンベルク型の相互作用が現れる．それぞれの核に対して (242) のゲージ変換を行うと，回転系における全ハミルトニアンは

$$\begin{aligned} H &= -\hbar\omega_{11}\left(\cos\varphi_1\frac{\sigma_{1x}}{2} + \sin\varphi_1\frac{\sigma_{1y}}{2}\right) - \hbar\omega_{12}\left(\cos\varphi_2\frac{\sigma_{2x}}{2} + \sin\varphi_2\frac{\sigma_{2y}}{2}\right) \\ &\quad + 2\pi J\frac{\sigma_z \otimes \sigma_z}{4} \end{aligned} \tag{246}$$

で与えられる．ただし $\sigma_{1x,y} = \sigma_{x,y} \otimes I$ および $\sigma_{2x,y} = I \otimes \sigma_{x,y}$ で J はスピン間相互作用の強さを表す．1量子ビットの場合と同様，共鳴条件 $\omega_{\rm irf} = \omega_{i0}$ をとった．ここで相互作用が Ising 型になっているが，これは回転系で見た場合，2つの核の回転数が数百 MHz 異なるため，$\sigma_{x,y} \otimes \sigma_{x,y}$ は平均して消えてしまうからである．z 成分 $\sigma_z \otimes \sigma_z$ は xy 軸周りに回転しても変化しないので，この項だけが残る．

各分子にスピン 1/2 の核が n 個ある場合は

$$\sigma_k^i = I \otimes I \otimes \ldots \otimes \overset{i\text{番目}}{\sigma_k} \otimes \ldots \otimes I \quad (k = x, y, z)$$

としてハミルトニアン (246) を一般化すると

$$H = -\hbar \sum_{i=1}^{n} \omega_{1i} \left(\cos\varphi_i \frac{\sigma_{ix}}{2} + \sin\varphi_i \frac{\sigma_{iy}}{2} \right) + 2\pi \sum_{i=1}^{n-1} J_{i,i+1} \frac{\sigma_{iz} \otimes \sigma_{(i+1)z}}{4} \tag{247}$$

が得られる．ただし核は1次元的に並び，最近接スピン間の相互作用しか無いものとする．実際はそれ以外の結合があり，スピンはネットワークを作る可能性もある．

前と同様ハミルトニアン (247) も $\mathrm{tr}H = 0$ を満たすので NMR 量子コンピュータは $\mathrm{SU}(2^n)$ に属するゲートしか実装できないが，量子力学では全体の位相は意味がないのでこれは制限にはならない．

9.1.3 擬純粋状態

NMR 量子コンピュータは室温で液体状態にある分子を量子計算に用いるので初期状態はさまざまなスピン状態の熱平衡状態になっている．したがって，あるアルゴリズム U を作用させたものも，様々な状態から得られる状態が混じったものになっている．このような状況で基底状態 $|00\rangle$ の寄与のみを取り出すにはいくつかの方法があるが，ここでは以下に述べる時間平均法を用いる [13].

まず温度 T の熱平衡状態を考えよう．その密度行列は

$$\begin{aligned} \rho_0 &= \exp(-H/k_BT)/Z(T) \\ &= \frac{1}{4} I_4 + \frac{1}{8k_BT} \begin{pmatrix} \hbar\omega_1 + \hbar\omega_2 & 0 & 0 & 0 \\ 0 & -\hbar\omega_1 + \hbar\omega_2 & 0 & 0 \\ 0 & 0 & \hbar\omega_1 - \hbar\omega_2 & 0 \\ 0 & 0 & 0 & -\hbar\omega_1 - \hbar\omega_2 \end{pmatrix} \\ &\equiv \mathrm{diag}(a, b, c, d) \end{aligned} \tag{248}$$

で与えられる．a, b, c, d は最後の式で定義される実数であり，それぞれ 1/4 に非常に近い．a は熱平衡状態における $|00\rangle$ の分布の割合を表す．次に熱平衡状態にあるゲート V を作用させ，系の密度行列を $\rho_0 \to V\rho_0 V^\dagger$ に変化させる．V として $U_{\rm cp} = \mathrm{CNOT}_{12}\mathrm{CNOT}_{21}$ をとる．ただし CNOT_{ij} は i を制御ビット，j をターゲットビットとする CNOT ゲートである．具体的には $\mathrm{CNOT}_{12} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_x, \mathrm{CNOT}_{21} = I \otimes |0\rangle\langle 0| + \sigma_x \otimes |1\rangle\langle 1|$ で表される．これにより，密度行列は

$$\rho_1 = U_{\rm cp}\rho_0 U_{\rm cp}^\dagger = \mathrm{diag}(a, d, b, c) \tag{249}$$

となる．同様に熱平衡状態に $U_{\rm cp}^2 = {\rm CNOT}_{21}{\rm CNOT}_{12}$ を作用させると密度行列は

$$\rho_2 = U_{\rm cp}^2 \rho_1 U_{\rm cp}^{2\dagger} = {\rm diag}(a,c,d,b) \tag{250}$$

となる．これらの3種類の密度行列で記述される系を用意し，独立にアルゴリズム U を実行させてその結果を平均すると，事実上密度行列

$$\rho_{\rm eff} \equiv \frac{1}{3}(\rho_0+\rho_1+\rho_2) = {\rm diag}(a,e,e,e) = eI_4 + (a-e){\rm diag}(1,0,0,0) \tag{251}$$

の系で量子アルゴリズム U を実行することと同等となる．ここに $e \equiv (b+c+d)/3$ である．eI_4 の部分はスペクトルには寄与せず，「上澄み」の $a-e$ の部分が $|00\rangle$ 状態を初期状態とした寄与を与える．

擬純粋状態を作る方法には，ここで述べた時間平均法以外にも空間平均法などがあるが，いずれにせよ平均操作を含み，その段階でユニタリー性が損なわれる．また量子ビットの数が増えていくと平均をとるための操作が増えるので，指数関数的な加速が損なわれる．これらの点から擬純粋状態を用いたNMR量子コンピュータは本当の量子コンピュータではないという批判がある．しかし手軽に量子アルゴリズムが実行できるという点では，とても魅力的な系である．

9.2　量子ゲートの実装

前節のハミルトニアンを用いて具体的に量子ゲートを構成しよう．

9.2.1　1量子ビットゲート

まず，ハミルトニアン (244) を用いて1量子ビットのゲートを実装することを考えよう．(244) は SU(2) の3つの生成子 $\sigma_k/2, (k=x,y,z)$ のうち $\sigma_{x,y}/2$ しか含まないので，注意が必要である．ここでは次の公式を利用しよう (補題 5.2 参照)：

$$\begin{aligned} U &= e^{-i\alpha\sigma_x/2}e^{-i\beta\sigma_y/2}e^{-i\gamma\sigma_x/2} \\ &= \begin{pmatrix} \cos\frac{\beta}{2}\cos\frac{\alpha+\gamma}{2} - i\sin\frac{\beta}{2}\sin\frac{\alpha-\gamma}{2} & -\sin\frac{\beta}{2}\cos\frac{\alpha-\gamma}{2} - i\cos\frac{\beta}{2}\sin\frac{\alpha+\gamma}{2} \\ \sin\frac{\beta}{2}\cos\frac{\alpha-\gamma}{2} - i\cos\frac{\beta}{2}\sin\frac{\alpha+\gamma}{2} & \cos\frac{\beta}{2}\cos\frac{\alpha+\gamma}{2} + i\sin\frac{\beta}{2}\sin\frac{\alpha-\gamma}{2} \end{pmatrix}. \end{aligned} \tag{252}$$

例えば Hadamard ゲート

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

を実現することを考えよう．$\det H = -1$ であるから，NMR量子コンピュータではそれと同値な

$$\tilde{H} = \frac{i}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in SU(2) \tag{253}$$

を実現する．H と $\tilde{H}$ の差は全体の位相だけであるから，この差は問題ではない．すると (252) と (253) を比べて $\alpha=0,\beta=-\pi/2,\gamma=-\pi$ ととればよいことが分かる．このパルス列を

$$-\mathtt{Ym}-\mathtt{XmXm}- \tag{254}$$

と表す．時間は左から右に流れている．ここで

$$\mathtt{X}=e^{i\pi\sigma_x/4},\mathtt{Y}=e^{i\pi\sigma_y/4},\mathtt{Xm}=e^{i\pi\sigma_x/4},\mathtt{Ym}=e^{i\pi\sigma_y/4} \tag{255}$$

はそれぞれ x (y) 軸周りの $\pi/2$ $(-\pi/2)$ 回転を表す．したがって XmXm は x 軸周りの $-\pi$ 回転を表す．

9.2.2 2量子ビットゲート

次に2量子ビット・ゲートの実現を考えよう．ハミルトニアン (246) には SU(4) の $4^2-1=15$ 個の生成子のうち5個しか含まれないので，上と同様の注意が必要である．このとき (252) に対応する分解は，以下の Cartan 分解である．SU(4) のリー代数を $\mathfrak{su}(4)$ で表す．その生成子にパウリ行列を用いて

$$\mathfrak{su}(4)=\mathrm{Span}\left(i\sigma_j/2\otimes I, iI\otimes\sigma_j/2, i\sigma_j\otimes\sigma_k/4\right) \tag{256}$$

とかく．Span( ) はその中にある生成子が張るベクトル空間の意味である．$i\sigma_j/2\otimes I, iI\otimes\sigma_j/2$ がそれぞれ3個，$i\sigma_j\otimes\sigma_k/4$ が9個で全部で15次元となることが直ちに分かる．ここで

$$\mathfrak{k}=\mathrm{Span}\left(i\sigma_j/2\otimes I, iI\otimes\sigma_j/2\right),\ \mathfrak{p}=\mathrm{Span}\left(i\sigma_j\otimes\sigma_k/4\right) \tag{257}$$

とおく．するとこれらは交換関係

$$[\mathfrak{k},\mathfrak{k}]\subset\mathfrak{k},\ [\mathfrak{p},\mathfrak{k}]\subset\mathfrak{p},\ [\mathfrak{p},\mathfrak{p}]\subset\mathfrak{k} \tag{258}$$

を満たすことが直ちに分かる．この交換関係を満たす分解 $\mathfrak{g}=\mathfrak{k}\oplus\mathfrak{p}$ をリー代数 $\mathfrak{g}$ の Cartan 分解という．

では，対応するリー群の分解はどうだろうか？$K=e^{\mathfrak{k}}$，$P=e^{\mathfrak{p}}$ とおくと，任意の $U\in\mathrm{SU}(4)$ にたいし

$$U=kp, k\in K, p\in P \tag{259}$$

が成り立つ．あきらかに $K=\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ である．さらに $\mathfrak{p}$ の中の最大可換部分代数を $\mathfrak{h}$ とし，$H=e^{\mathfrak{h}}$ とすると $k_1\in K, h\in H$ が存在して $p=k_1^\dagger hk_1$ と書くことができる．$\mathfrak{h}$ を Cartan 部分代数，可換群 H を Cartan 部分群という．具体的に

$$\mathfrak{h}=\mathrm{Span}(i\sigma_j\otimes\sigma_j/4) \tag{260}$$

で与えられる．これらの生成子が可換であることは各自確かめられたい．したがって SU(4) の Cartan 分解

$$U=k_2hk_1, k_i\in K, h\in H \tag{261}$$

が成立する．

具体的に k_i, h を求める方法を述べる．それには Binary 基底 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ から Bell 基底

$$\begin{aligned} |\Psi_0\rangle &= (1/\sqrt{2})(|00\rangle + |11\rangle),\ |\Psi_1\rangle = (i/\sqrt{2})(|01\rangle + |10\rangle), \\ |\Psi_2\rangle &= (1/\sqrt{2})(|01\rangle - |10\rangle),\ |\Psi_3\rangle = (i/\sqrt{2})(|00\rangle - |11\rangle). \end{aligned} \tag{262}$$

に移るのが便利である．[12]この基底の変換に伴い，行列 U は $U \to U_B \equiv Q^\dagger U Q$ と変換される．ただし

$$Q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & i & -1 & 0 \\ 1 & 0 & 0 & -i \end{pmatrix}. \tag{263}$$

Q は以下の重要な性質を持つ：

(1) 行列 Q は $K = \mathrm{SU}(2) \otimes \mathrm{SU}(2)$ と $\mathrm{SO}(4)$ の間の同型を定義する．すなわち $k \in K$ にたいし $Q^\dagger k Q \in \mathrm{SO}(4)$.

(2) 行列 Q は Cartan 部分群を対角化する．すなわち $h \in H$ にたいし

$$Q^\dagger h Q = \mathrm{diag}(e^{i\theta_0}, e^{i\theta_1}, e^{i\theta_2}, e^{i\theta_3}).$$

これらは直接の計算で確かめられる．これから $U = k_2 h k_1$ と分解されると

$$U_B = Q^\dagger U Q = Q^\dagger k_2 Q \cdot Q^\dagger h Q \cdot Q^\dagger k_2 Q = O_2 h_D O_1, \tag{264}$$

ただし $O_i \equiv Q^\dagger k_i Q \in \mathrm{SO}(4)$ で $h_D \equiv Q^\dagger h Q$ は対角行列．さらに $U_B^T U_B = O_1^T h_D^2 O_1$ から O_1 は $U_B^T U_B$ を対角化し，その固有値は h_D^2 の対角成分であることが分かる．最後に $O_2 = U_B (h_D O_1)^{-1}$ より O_2 が求められる．

量子系はデコヒーレンスという性質を持ち，それを克服するにはできるだけ早く計算を終えることが望ましい．以前注意したように，Barenco *et al* の Universality 定理 (定理 5.1) では，U(2) ゲートと CNOT ゲートがユニバーサルであることを主張しているが，それらが様々なリソースの点で最適であることは主張していない．変分原理的な考えをすれば，使うゲートの可能性を広げれば広げるほどリソースを節約する解が求められるはずである．以下 Cartan 分解を使って時間最適解の求め方を議論しよう．NMR を含む一般の量子コンピュータにおいて，1 量子ビットゲートの実行時間は 2 量子ビットゲートのものよりもかなり早い．実際量子ビット間の結合の強さを J とすると，2 量子ビットゲートの実行時間は $T \sim 1/J$ となる．もし J が非常に大きければ，各量子ビットは 1 個の量子ビットとしての個性を失ってしまう．NMR で言えば，K に属する 1 量子ビット操作は $\sim 10\mu$s 程度で実行されるが，$J \sim 100$Hz なので 2 量子ビット操作には ~ 10ms 程度の時間がかかる．したがって，ある量子ゲートの実行時間を最小にするには $U = k_2 h k_1$ において h を実現するのに必要な時間を最小にすればよいことが分かる．K の元は好きなときに好きなだ

[12](80) とは位相が異なるが，ここではこちらが便利である．

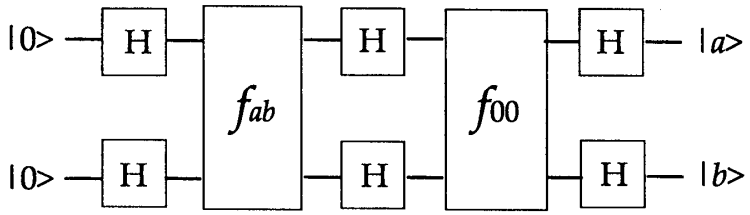


図 24: Grover のアルゴリズムの量子回路．H は Hadamard ゲート，f_{ab} は選択的回転ゲートである．

け使うことができる．元 h が

$$h = Qh_DQ^\dagger = \exp\left[-i\sum_{j=x,y,z}\alpha_j(\sigma_j\otimes\sigma_j/4)\right]$$

と表されたとしよう．ハミルトニアン (246) と比べると

$$\frac{1}{4}\sum_{j=x,y,z}|\alpha_j| = \frac{\pi}{2}JT \tag{265}$$

に対応していることが分かる．T はこの分解によるアルゴリズムの実行時間である．h_D^2 から h_D を求めるときに分岐の取り方の不定性が生じるが，時間最適解では，分岐は (265) の左辺が最小になるように選ばなければならない．

9.3 例：2 量子ビット Grover のアルゴリズム

Cartan 分解による時間最適解の例として 2 量子ビットの Grover のアルゴリズムを考えよう [14]．これは図 24 の量子回路で与えられる．ここに H は Hadamard ゲート，f_{ab} は選択的回転ゲートで

$$\begin{aligned} f_{ab}: &\ |ab\rangle \mapsto -|ab\rangle \\ :&\ |cd\rangle \mapsto |cd\rangle \quad (cd)\neq(ab) \end{aligned}$$

で与えられる．例として Grover のアルゴリズムのうち $|00\rangle$ を入力として，$|10\rangle$ を出力とするゲート U_{10} を考える．前に述べたように，熱平衡分布から $|00\rangle$ を初期状態とする寄与を取り出すには，擬純粋状態の処方箋に従って熱平衡状態に U_{10} 以外に独立に $U_{10\mathrm{a}}\equiv U_{10}U_{\mathrm{cp}}, U_{10\mathrm{b}}\equiv U_{10}U_{\mathrm{cp}}^2$ も作用させ，得られる 3 つのスペクトルを平均すればよい [13]．結果は

$$U_{10}=\begin{pmatrix} 0 & 1 & 0 & 0\\ 0 & 0 & 0 & -1\\ -1 & 0 & 0 & 0\\ 0 & 0 & -1 & 0 \end{pmatrix}, U_{10\mathrm{a}}=\begin{pmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\\ -1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0 \end{pmatrix}, U_{10\mathrm{b}}=\begin{pmatrix} 0 & 0 & 1 & 0\\ 0 & -1 & 0 & 0\\ -1 & 0 & 0 & 0\\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{266}$$

で与えられる．

前節の処方箋に従いこれらの行列の Cartan 分解を行う [14]. 最適解の例は

$$\begin{aligned} U_{10} &: k_1 = I,\ h = e^{i(\pi/4)(\sigma_x\otimes\sigma_x-\sigma_y\otimes\sigma_y)},\ k_2 = e^{-i(\pi/4)\sigma_z}\otimes e^{i(\pi/2\sqrt{2})(\sigma_x+\sigma_y)} \\ U_{10a} &: k_1 = I_2\otimes e^{-i(\pi/4)\sigma_x},\ h = e^{-i(\pi/4)\sigma_z\otimes\sigma_z},\ k_2 = e^{i(\pi/2)\sigma_y}\otimes e^{i(\pi/3\sqrt{3})(\sigma_x+\sigma_y+\sigma_z)} \\ U_{10b} &: k_1 = e^{-i(\pi/3\sqrt{3})(\sigma_x+\sigma_y+\sigma_z)}\otimes I_2,\ h = e^{-i(\pi/4)\sigma_z\otimes\sigma_z},\ k_2 = e^{i(\pi/4)\sigma_x}\otimes I_2. \end{aligned} \quad (267)$$

表 1 はこれらの結果を NMR のパルス列で表したものである. ここでハミルトニアン (246) に含まれない項は, たとえば

$$e^{i(\pi/4)(\sigma_x\otimes\sigma_x)} = [e^{i(\pi/4)\sigma_x}\otimes e^{-i(\pi/4)\sigma_y}]e^{i(\pi/4)(\sigma_z\otimes\sigma_z)}[e^{-i(\pi/4)\sigma_x}\otimes e^{i(\pi/4)\sigma_y}].$$

などを用いて手持ちの生成子で書き直した.

通常のパルス列 [13]		
ゲート	パルス列	実行時間
U_{10}	1: -Y -(1/2J)-Ym-Xm-(1/2J)-Ym-Xm- 2: -Y -(1/2J)-Ym-X -(1/2J)-Ym-Xm-	$1/J$
$U_{10}U_{cp}$	1: -X -(1/2J)-X ----------Y -(1/2J)-Ym-Xm-(1/2J)-Ym-Xm- 2: ----------X -(1/2J)-X -Y -(1/2J)-Ym-X -(1/2J)-Ym-Xm-	$2/J$
$U_{10}U_{cp}^2$	1: ----------X -(1/2J)-X -Y -(1/2J)-Ym-Xm-(1/2J)-Ym-Xm- 2: -X -(1/2J)-X ----------Y -(1/2J)-Ym-X -(1/2J)-Ym-Xm-	$2/J$
時間最適化されたパルス列 [14]		
ゲート	パルス列	実行時間
U_{10}	1: -X -(1/2J)-Xm-Ym-(1/2J)-Y -Pi(45)- 2: -X -(1/2J)-Xm-Y -(1/2J)-X -Ym -	$1/J$
$U_{10}U_{cp}$	1: -X -(1/2J)-Xm-Ym- 2: -Ym-Ym-	$1/2J$
$U_{10}U_{cp}^2$	1: 2: -Y -X -(1/2J)-Xm-	$1/2J$

表 1: Grover のアルゴリズムを実現するパルス列. 上の段は通常のパルス列 [13], 下の段は時間的に最適化されたパルス列 [14]. 1(2) は第 1(2) 量子ビットを表す. X (Xm) と Y (Ym) は x ($-x$) 軸, および y ($-y$) 軸回りの $\pi/2$ パルスを表す. Pi(45) は Bloch 球で $(1,1,0)$ 回りの π パルス. 通常のパルス列に比べ最適化されたパルス列では全パルス数が 38 から 18 に, 全実行時間が $5/J$ から $2/J$ に減少している.

実験では ^{13}C で置換した chloroform の H と ^{13}C を量子ビットとして用い, JEOL ECA-500 NMR 装置で核スピン制御を行った. 図 25 は $|00\rangle$ に U_{10} を作用させ $|10\rangle$ の位置にある ^{13}C のスペクトルを測定した結果である. ピークが負であることから ^{13}C 核は状態 $|1\rangle$ にあり, ピークの位置が 77.5 ppm にあることから H 核は $|0\rangle$ 状態にあることが分かる. 挿入図は H 核が $|1\rangle$ 状態にあれば現れるスペクトル付近 (79.2 ppm) を測定したものである. (a) では 1 量子ビットの $\pi/2$ 回転に 25 μs のパルス幅を用いた. (b) では故意にパルス幅を長く取り 250 μs とした. 破線は [13] の通常のパルス列の結果を, 実線は我々の時間最適パルス列の結果を測定したものである. (a) では両者の差があまり明白ではないが, (b) では最適化されたパルス列のほうがよりシャープなピークを与え, $|11\rangle$ におけるノイズも減少していることが分かる. 実際, 最適化によりパルス数は 38 から 18 に, 全実行時間は $5/J$ から $2/J$ に減少しており, その効果が見えていると思われる.

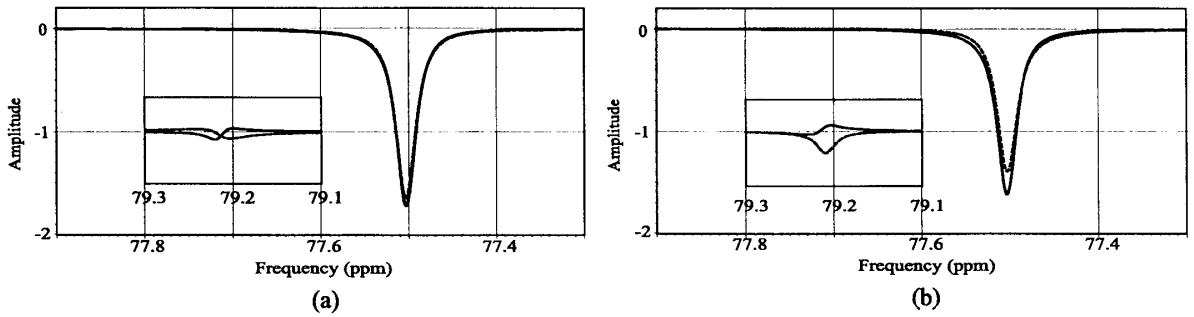


図 25: U_{10} を実行後に測定した $|10\rangle$ 状態を示すスペクトル．破線は通常のパルス列 [14]，実線は時間的に最適化されたパルス列 [15] を用いた測定結果．(a) では 1 量子ビットを $\pi/2$ 回転させるのに 25μs，(b) では 250μs のパルス幅を用いた．各挿入図は $|11\rangle$ の位置に現れるノイズを示す．

謝辞

京都大学大学院理学研究科で集中講義をする機会を与えていただいた水崎隆雄氏，またその講義ノートを物性研究に掲載するよう薦めていただいた北村光氏に感謝します．2000 年の「中部地方素粒子論夏の学校」で量子計算の明解な講義をされ筆者をこの道に引き込まれた細谷暁夫氏，筆者の要望にこたえ NMR 量子計算機を立ち上げていただいた近藤康氏，常日頃さまざまな議論をしていただく谷村省吾氏にも感謝します．大学院生の平松崇君には原稿のミスプリを数多く指摘してもらいました．

参考文献

[1] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information*, (Cambridge University Press, Cambridge, 2000).

[2] 細谷暁夫「量子コンピュータの基礎」サイエンス社 (1999).

[3] 上坂吉則「量子コンピュータの基礎数理」コロナ社 (2000).

[4] E. Rieffel and W. Polak, ACM Computing Surveys **32**, (2000) 300.

[5] S.J. Lomonaco, eprint quant-ph/0007045, quant-ph/0010034 (2000).

[6] W.-H. Steeb, *Matrix Calculus and Kronecker Product with Applications and C++ Programs*, World Scientific, Singapore (1997).

[7] G. P. Berman, G. D. Doolen, R. Mainieri, and V. I. Tsifrinovich, *Introduction to Quantum Computers*, World Scientific, Singapore (1998).

[8] C.H. Bennett and G. Brassard, *Proceedings of the IEEE International Coference on Computer Systems and Signal Processing* (1984) 175.

[9] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, Phys. Rev. A **52** (1995), 3457.

[10] L. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computation* (ACM Press, New York, 1996), 212.

[11] L. K. Grover, Phys. Rev. Lett. **79** (1997) 325.

[12] R.L. Rivest, A. Shamir and L.M. Adleman, Comm. ACM, **21** (1978) 120.

[13] P. Shor, in Proceedings of the 35th Annual Symposium on Foundation of Computer Science, IEEE Computer Society Press, Los Alamits, CA (1994) 116.

[14] I. L. Chuang, N. Gershenfeld, and M. Kubinec, Phys. Rev. Lett. **80** (1998) 3408.

[15] M. Nakahara, Y. Kondo, K. Hata and S. Tanimura, Phys. Rev. A **70** (2004) 052319.